NCS TIB 87-10

NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 87-10

COMPUTER SIMULATION OF GROUP 3 FACSIMILE ENCRYPTION

MARCH 1987

NATIONAL COMMUNICATIONS SYSTEM

OFFICE OF THE MANAGER
WASHINGTON, D.C. 20305-2010

IN REPLY
REFER TO

NCS-TS

SEP 1 3 1988

Defense Technical Information Center
ATTN: DTIC-FDAC
Cameron Station
Alexandria, VA 22314-6145

Dear Mr. Proctor:

The enclosed Technical Information Bulletins are being returned to you as is for final processing. Per our telephone conversation, the pages in question are intentionally prepared to include poor facsimile tranmission examples.

for Donald D. Wilson
DENNIS BODSON
Assistant Manager
Technology & Standards

Unclassified
SECURITY CLASSIFICATION OF THIS PAGE

AD-A199330

REPORT DOCUMENTATION PAGE

Form Approved
OMB No 0704-0188

1a REPORT SECURITY CLASSIFICATION Unclassified	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) NCS-TIB-87-10	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Delta Information Systems, Inc 6b OFFICE SYMBOL (If applicable)	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State, and ZIP Code) Horsham Business Center, Bldg. 3 300 Welsh Road Horsham, PA 19044	7b ADDRESS (City, State, and ZIP Code)
8a NAME OF FUNDING SPONSORING ORGANIZATION National Communications System 8b OFFICE SYMBOL (If applicable) NCS-TS	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER DCA100-83-C-0047
8c ADDRESS (City, State, and ZIP Code) Office of Technology & Standards Washington, D.C. 20305-2010	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO: 33127K PROJECT NO: TASK NO: P00010/8 WORK UNIT ACCESSION NO:
11 TITLE (Include Security Classification) Computer Simulation of Group 3 Facsimile Encryption	
12 PERSONAL AUTHOR(S)	
13a TYPE OF REPORT Final 13b TIME COVERED FROM ____ TO ____	14 DATE OF REPORT (Year, Month, Day) March 1987 15 PAGE COUNT 70
16 SUPPLEMENTARY NOTATION	

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Group 3 Facsimile Encryption

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The purpose of this study was to determine the error sensitivity of Group 3 facsimile systems in which the (DES) encryption algorithm is employed to provide the secure transmission of binary documents. This report presents the results of a computer simulation study in which the effects of transmission errors on the performance of Group 3 facsimile employing the DES encryption algorithm were examined. Section 1 provides a brief description of the objectives of the study and contains a symposis that outlines the results and conclusions obtained. Section 2 presents the technical approach employed in the study and includes a discussion of the system analysis performed, the simulation methodology employed, and detailed descriptions of the compression, encryption, and error signal algorithms simulated. The results of the simulation study are presented in Section 3. The conclusions made based on these reults are contained in Section 4.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL J. Orndorff	22b TELEPHONE (Include Area Code) 202-692-2124 22c OFFICE SYMBOL NCS-TS

DD Form 1473, JUN 86 Previous editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

NCS TECHNICAL INFORMATION BULLETIN 87-10

COMPUTER SIMULATION OF GROUP 3 FACSIMILE ENCRYPTION

PROJECT OFFICER

Dennis Bodson

DENNIS BODSON
Senior Electronics Engineer
Office of NCS Technology
and Standards

APPROVED FOR PUBLICATION:

Dennis Bodson

DENNIS BODSON
Assistant Manager
Office of NCS Technology
and Standards

FOREWORD

Among the responsibilities assigned to the Office of the Manager, National Communications System, is the management of the Federal Telecommunication Standards Program. Under this program, the NCS, with the assistance of the Federal Telecommunication Standards Committee identifies, develops, and coordinates proposed Federal Standards which either contribute to the interoperability of functionally similar Federal telecommunication systems or to the achievement of a compatible and efficient interface between computer and telecommunication systems. In developing and coordinating these standards, a considerable amount of effort is expended in initiating and pursuing joint standards development efforts with appropriate technical committees of the Electronics Industries Association, the American National Standards Institute, the International Organization for Standardization, and the International Telegraph and Telephone Consultative Committee of the International Telecommunication Union. This Technical Information Bulletin presents an overview of an effort which is contributing to the development of compatible Federal, national, and international standards in the area of Facsimile. It has been prepared to inform interested Federal activities of the progress of these efforts. Any comments, inputs or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

Office of the Manager
National Communications System
ATTN: NCS-TS
Washington, DC 20305-2010

COMPUTER SIMULATION OF
GROUP 3 FACSIMILE ENCRYPTION

March, 1987

Final Report

Submitted to:

NATIONAL COMMUNICATIONS SYSTEM

Office of Technology and Standards

Washington, DC 20305

Contracting Agency:

DEFENSE COMMUNICATIONS AGENCY

Contract Number - DCA100-83-C-0047

Modification/Task Number - P00010/8

D E L T A I N F O R M A T I O N S Y S T E M S, I N C.

Horsham Business Center, Bldg. 3

300 Welsh Road

Horsham PA 19044

Table of Contents

1.0 INTRODUCTION

This document summarizes work performed by Delta Information Systems, Inc., for the Office of Technology and Standards of the National Communications System, an organization of the U.S. Government, headed by National Communications System Assistant Manager Dennis Bodson. Mr. Bodson is responsible for the management of the Federal Telecommunications Standards Program, which develops telecommunications standards, the use of which is mandatory for all Federal agencies. The purpose of this study, performed under Task 8 of Modification Number P00010 of contract number DCA100-83-C-0047, was to determine the error sensitivity of Group 3 facsimile systems in which the DES encryption algorithm is employed to provide the secure transmission of binary documents.

Federal Standards 1062 and 1063 define Group 3 facsimile apparatus and transmission procedures, respectively. The NCS recently established Federal Standard 1028, in which the use of the Data Encryption Standard (DES) to provide secure transmission over Group 3 facsimile equipment is defined. One of the key issues regarding the use of Group 3 facsimile is the sensitivity of the transmitted signal to data link errors. This report presents the results of a computer simulation study performed by Delta Information Systems in which the effects of transmission errors on the performance of Group 3 facsimile employing the DES encryption algorithm were examined.

This report is comprised of four sections. Section 1.0 provides a brief description of the objectives of the study and contains a synopsis that outlines the results and conclusions obtained. Section 2.0 presents the technical approach employed in the study and includes a discussion of the system analysis performed, the simulation methodology employed, and detailed descriptions of the compression, encryption, and error signal algorithms simulated. The results of the simulation study are presented in Section 3.0, and the conclusions made based on these results are contained in Section 4.0.

1.1 Synopsis

In this study, 48 simulations were performed in order to determine the effect of data link errors on the error sensitivity of secure Group 3 facsimile transmissions. The parametric variations employed in these simulations included two compression algorithms in the Group 3 encoding and decoding steps, Modified Huffman and Modified READ coding, two error signal types, single and double burst errors, two bit error rates, 4×10^{-3} and 1×10^{-3}, two error conditions, with and without encryption, and three test documents, CCITT documents #1, #5, and #7.

The Group 3 compression algorithms were derived from CCITT Recommendation T.4 (equivalent to Federal Standard 1062); the encryption/decryption algorithm, the Data Encryption Standard algorithm in the 1-bit cipher feedback mode, was derived from an analysis of Federal Standards 1027 and 1028 and FIPS publications

46 and 81. The error signal algorithms were derived from error sensitivity reports previously performed by Delta Information Systems.

The effects of transmission errors on secure Group 3 facsimile were found to be only slightly greater than their effects on Group 3 facsimile without encryption. The encryption process, while introducing a large number of errors into the encoded data stream, did not severely affect the image quality produced by secure Group 3 facsimile. On the average, the error sensitivity of the simulations in which encryption was employed was only 2% to 15% greater than in those runs in which it was not. The visual effect of the decryption process was noticeable only in small regions of the output images, and even then only in those images in which the higher bit error rate and the MRC algorithm was employed.

The simulation results indicated that the structure of the error signal had a significant effect on the error sensitivity; the number of errors within an error group, where an error group is either an error burst for single burst error signals or a disturbance (two bursts) for double burst error signals, had less of an effect on error sensitivity than the number of error groups present in an error signal. This explains why the single burst error signals had a greater effect on error sensitivity than the double burst errors; although there are more error bits per group in a double burst error signal (twice as many) at a given bit error rate, there are fewer error groups present (half as many).

It also explains why the decryption process had only a limited effect on error sensitivity. Although the decryption process causes a large expansion in the number of error bits in the encoded data stream ($\approx$10:1 for single burst error signals, $\approx$5:1 for double burst error signals), the errors remain localized to the area in which the data link error group is located, and the propagation of error bits in the decoded output image is modest.

2.0 TECHNICAL APPROACH

2.1 System Analysis

The sensitivity of Group 3 facsimile to data link errors has been previously studied by Delta Information Systems for the DCA (refs. 1, 2, 3). In this study, the effects of data link errors on secure Group 3 transmissions was evaluated. In order to develop computer software to simulate the secure transmission of documents with Group 3 equipment, it was first necessary to fully define the compression, encryption, and transmission characteristics of a secure Group 3 facsimile transmission. The Group 3 compression/decompression process was defined through an analysis of CCITT Recommendation T.4 (ref. 4). Federal Standards 1027 and 1028 (refs. 5, 6) and FIPS publications 46 and 81 (refs. 7, 8) were analyzed in order to determine the details of the encryption process employed. The error sensitivity studies previously performed by Delta Information Systems were used as a source of information regarding the types of data link errors common to Group 3 transmissions.

Figure 2.1 is a functional block diagram which illustrates the major steps involved in a secure Group 3 facsimile transmission. In the Group 3 encoder, each input document is compressed using either the Modified Huffman or the Modified READ coding algorithm; the output of the encoder is a data stream consisting of compressed scan lines, end-of-line (EOL) codes, and fill bits. The DES encryptor enciphers this data stream using the Data Encryption Standard (DES) algorithm in the 1-bit cipher

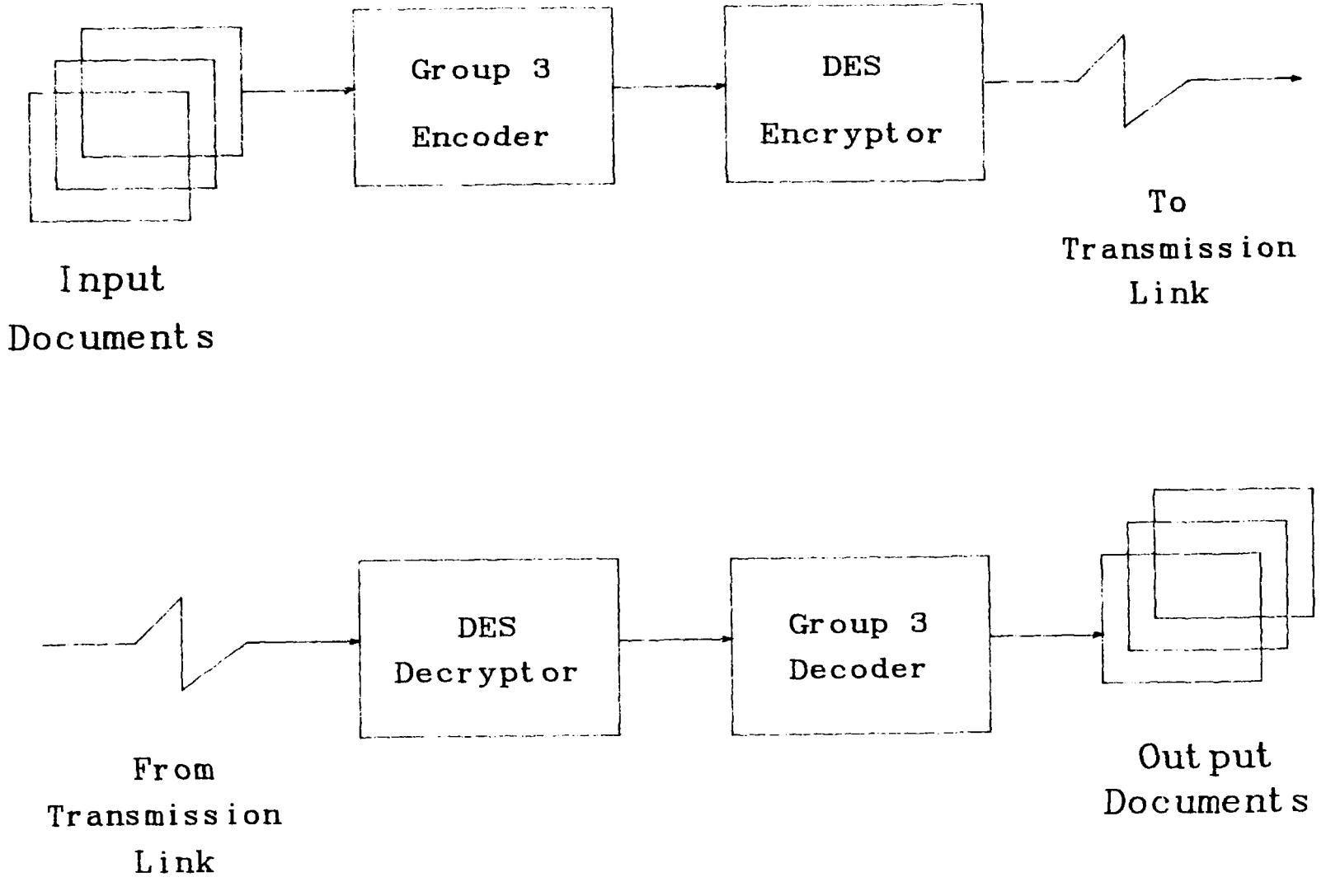


Figure 2.1 – Functional Block Diagram of a Secure Group 3 Transmission

feedback mode. The encoded and encrypted data is then sent across the transmission channel; assuming an error-free transmission (and assuming the same key variable is used in both the encryptor and the decryptor), the data is decrypted and decoded to produce an exact reproduction of the input document. Group 3 data links, however, are not generally error-free; they are subject to various types of error signals. In this study, two representative error signal types, single and double burst errors, were employed in order to determine the error sensitivity of secure Group 3 facsimile transmissions.

In evaluating the secure Group 3 facsimile transmission process, the first simulation method considered was to duplicate the process exactly; that is, create a software module for each of the functional blocks in Figure 2.1 and encode, encrypt, error corrupt, decrypt, and decode the test images. This method, while being the most direct, posed several problems. It does not take full advantage of the software written for the previous error sensitivity studies (refs. 1, 2, 3). It would require an excessive amount of computer processing time because the DES algorithm, which requires a significant amount of bit matrix manipulation, is invoked twice (once for encryption, once for decryption) for each bit in the encoded data stream (200,000 to 850,000 times). In addition, it would be highly inefficient in that it would be needlessly encrypting and decrypting large portions of the test documents that are not affected by the error signals.

The second method considered, and the one chosen to perform the simulation, avoids all of the aforementioned problems. It

employs the simulation software from the previous studies directly (with a few minor modifications to bring it up to date). It avoids the excessive computer processing time by applying the encryption/decryption process to the error signals rather than to the encoded data stream. In this way, only those areas of the document that contain errors are encrypted and decrypted, and the encryption/decryption process need only be applied once for each error signal type at each bit error rate, regardless of the number of simulation runs performed.

2.2 Simulation Methodology

Figure 2.2 is a block diagram of the software developed to implement the simulation method selected in the system analysis task. The encoder, error insertion, and decoder modules are contained in a single program, an updated version of the program used in the previous error sensitivity studies. This program encodes a document, corrupts the coded data by placing errors at positions read in from an error position file, and decodes the corrupted data to produce an output image containing errors. The program also outputs various compression and error sensitivity statistics, such as the number of compressed bits, the number of error bits inserted, the error sensitivity factor, etc.

Software modules not depicted in Figure 2.2 were written to generate error position files that simulate the two error signal types chosen for evaluation. The program that generates the double burst error position files was obtained from a previous error sensitivity study (ref. 3); the program that generates the

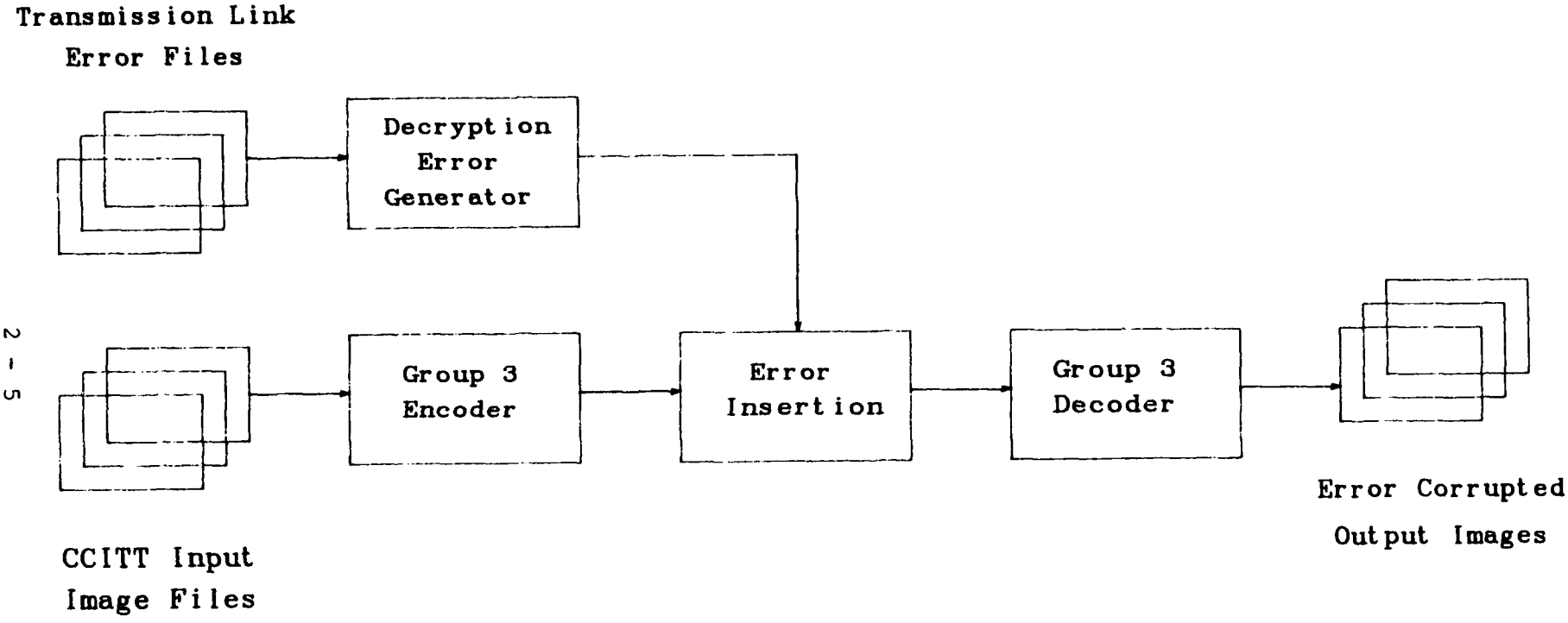


Figure 2.2 – Simulation Software Block Diagram

single burst error position files was developed as a modification of the double burst error program. The decryption error generator module shown in Figure 2.2 reads in an error position file, adds the errors that would be caused by the decryption process, and outputs a new error position file that simulates the error pattern of a decrypted coded data stream that contains transmission errors.

In performing the simulations associated with this study, the following steps were taken.

1. The double burst error generation program was run twice in order to produce double burst error position files at the two selected bit error rates.
2. The single burst error generation program was also run twice in order to produce single burst error position files at the two selected bit rates.
3. The decryption error generator program was then applied to each of these four error position files to produce four more error position files that contained errors due to decryption in addition to data link errors.
4. The program that performs the encoding, error insertion, and decoding steps was then run a total of 48 times, using the three test documents and the eight error position files mentioned above.

2.2.1 The Decryption Error Generator Module

The simulation of the DES encryption/decryption process was the main task involved in the software development effort; Figure 2.3 is a functional block diagram of the process. As stated earlier, a direct simulation of the process was possible but not practical; because of the intensive bit matrix manipulations required by the DES algorithm (ref. 7), the computer time needed to perform the 48 simulation runs would have been prohibitive. The technique employed to simulate the effects of the encryption/decryption process on secure Group 3 facsimile transmissions significantly reduced the amount of computer time required to perform the simulations. This was accomplished by applying the DES algorithm to the error signals rather than the images themselves.

The simulation technique takes advantage of the fact that, although the actual encrypted bit stream is highly unpredictable (the primary purpose of the DES algorithm), the effects of transmission errors on secure Group 3 facsimile transmissions are not. The effects of the encryption/decryption process manifest themselves in the decryption step, as this is the first step taken after the introduction of transmission errors. The decryption error generator software simulates the decryption of an encrypted bit stream containing errors by taking a simulated error signal and adding to it the errors that would be generated by the decryption process.

In the decryption error generator software module, the input bit stream is a sequence of correct bits (0's) interspersed with

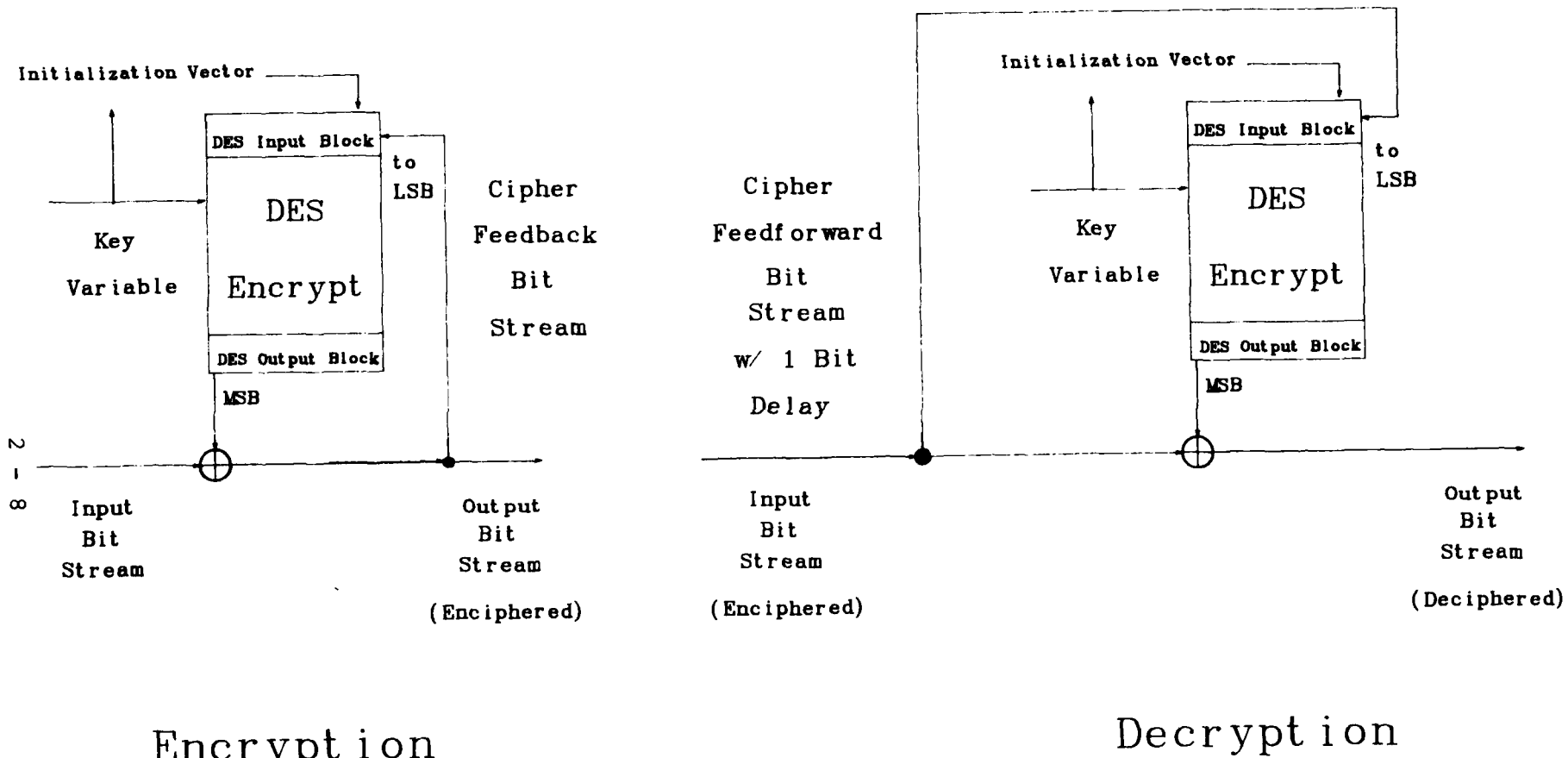


Figure 2.3 – Functional Block Diagram of the Encryption/Decryption Process

groups of incorrect bits (1's) that represents a simulated error signal (see Figure 2.4). The DES encryption algorithm is first run with an input block consisting of all 0's (which represents an input block containing no errors) in order to determine the true value of the most significant bit (MSb) of the DES output block. The simulated error signal is then processed as follows. When an error bit is encountered, the DES encryption algorithm is initiated and the MSB of the DES output block is determined. This MSB is then compared with the true value of the MSB; if the MSB is equivalent to the true MSB, the MSB is set to 0 (correct); otherwise, it is set to 1 (incorrect).

The MSB is then exclusive-ORed with the input bit to form an output error signal bit. The input bit is fed forward to the LSB of the DES input block, which is left-shifted to accommodate the input bit, and the above sequence of steps is repeated. This process continues until the entire error group completely passes through the DES input block. The decryption error generator module then repeats this procedure for every error group in the simulated error signal, producing a new simulated error signal in which the error propagation due to the decryption process is incorporated.

This simulation process is actually a close approximation of the decryption of a corrupted cipher bit stream rather than an exact representation. The simulation process assumes that the error propagation due to the decryption process is independent of the content of the data stream. In actuality, the error pattern produced by the decryption of a corrupted cipher bit stream is dependent upon the data.

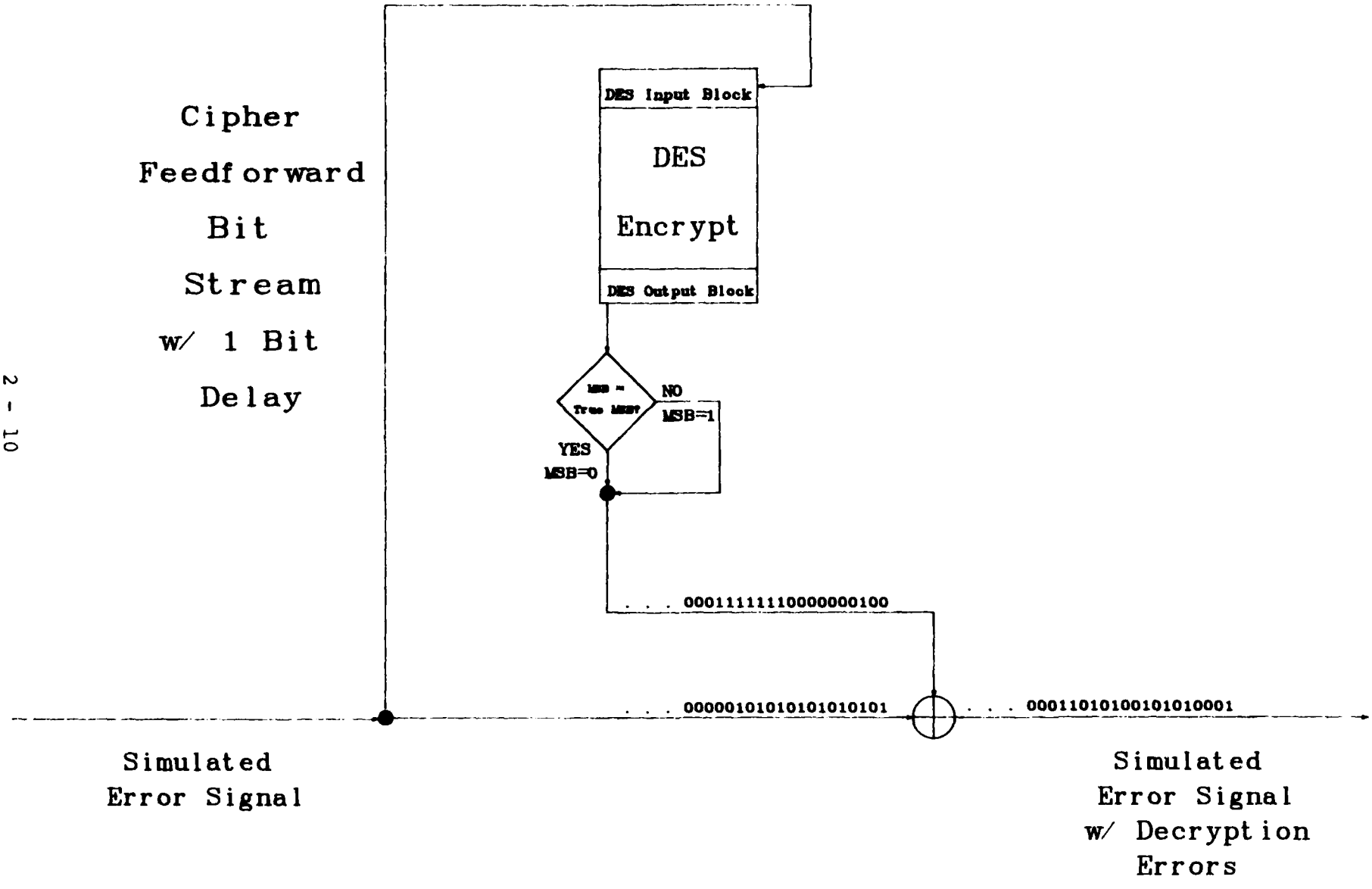


Figure 2.4 – Functional Block Diagram for Decryption Error Generator Module

The validity of the assumption lies in the fact that the length of the error group after the decryption process is independent of the data stream; only the exact error pattern and the number of errors within the error group are dependent upon the data stream. Because the length of the expanded error group is data independent, and the number of errors in an error group has much less of an effect on error sensitivity than the number of error groups present, a close approximation of the effect of transmission errors on Group 3 facsimile with encryption can be achieved by employing an "average" error propagation pattern. By making this assumption, the computational complexity of the simulation was greatly reduced.

The sample error signal in Figure 2.4, a double burst error group, illustrates the simulation process. As stated earlier, each incorrect bit is represented by a 1 and each correct bit is represented by a 0. The input error signal is both exclusive-ORed with the MSB stream from the DES output block and fed forward (with a 1 bit delay) to the DES input block. In exclusive-ORing the input error signal with the DES MSB stream, an incorrect bit in the output error signal can be caused by an incorrect bit in either stream; however, incorrect bits in both streams cancel each other and produce a correct bit in the output error signal (e.g. bit positions 3, 11, 13, and 15 in the example). The number of error bits in the output error signal caused by the decryption process is much larger than the number of error bits in the input error signal because each error group remains in the DES input block for 70 to 95 iterations, depending on the error type.

2.3 Algorithm Descriptions

2.3.1 Group 3 Compression

Documents are encoded in one of two ways in Group 3 facsimile systems. The one-dimensional encoding algorithm represents all of the runs of consecutive black and/or white pels along a scan line with code words obtained from the Modified Huffman code tables (see Tables 2.1, 2.2, and 2.3). The two-dimensional encoding algorithm is an optional extension of the 1D algorithm that increases compression by taking advantage of the vertical correlation between pels.

The one-dimensional run-length coding process, also known as Modified Huffman coding (MHC), compresses a document by representing the actual sequence of bits along a scan line with a series of variable length code words. Run lengths between 0 and 63 pels are encoded with the corresponding code words from Table 2.1; these code words are called terminating codes because they are the final part of the code sequence used to represent a pel run length. A run length between 64 and 1728 pels is encoded with a make-up code from Table 2.2 and a terminating code from Table 2.1 (e.g. a run of 1609 white pels would be encoded with the code sequence [010011010][10100]); Table 2.3 contains make-up codes for run lengths longer than 1728 pels (for Group 3 facsimile equipment that can accommodate larger documents).

A Group 3 transmission is comprised of three types of data; coded scan line data, end of line (EOL) codes, and fill bits.

Terminating codes

White run length	Code word	Black run length	Code word
0	00110101	0	0000110111
1	000111	1	010
2	0111	2	11
3	1000	3	10
4	1011	4	011
5	1100	5	0011
6	1110	6	0010
7	1111	7	00011
8	10011	8	000101
9	10100	9	000100
10	00111	10	0000100
11	01000	11	0000101
12	001000	12	0000111
13	000011	13	00000100
14	110100	14	00000111
15	110101	15	000011000
16	101010	16	0000010111
17	101011	17	0000011000
18	0100111	18	0000001000
19	0001100	19	00001100111
20	0001000	20	00001101000
21	0010111	21	00001101100
22	0000011	22	00000110111
23	0000100	23	00000101000
24	0101000	24	00000010111
25	0101011	25	00000011000
26	0010011	26	000001001010
27	0100100	27	000001001011
28	0011000	28	000001001100
29	00000010	29	000001001101
30	00000011	30	000001101000
31	00011010	31	000001101001
32	00011011	32	000001101010
33	00010010	33	000001101011
34	00010011	34	000011010010
35	00010100	35	000011010011
36	00010101	36	000011010100
37	00010110	37	000011010101
38	00010111	38	000011010110
39	00101000	39	000011010111
40	00101001	40	000001101100
41	00101010	41	000001101101
42	00101011	42	000011011010
43	00101100	43	000011011011
44	00101101	44	000001010100
45	00000100	45	000001010101
46	00000101	46	000001010110
47	00001010	47	000001010111
48	00001011	48	000001100100
49	01010010	49	000001100101
50	01010011	50	000001010010
51	01010100	51	000001010011
52	01010101	52	000000100100
53	00100100	53	000000110111
54	00100101	54	000000111000
55	01011000	55	000000100111
56	01011001	56	000000101000
57	01011010	57	000001011000
58	01011011	58	000001011001
59	01001010	59	000000101011
60	01001011	60	000000101100
61	00110010	61	000001011010
62	00110011	62	000001. 0110
63	00110100	63	000001100111

Table 2.1 - MHC Terminating Code Table

Make-up codes

White run lengths	Code word	Black run lengths	Code word
64	11011	64	0000001111
128	10010	128	000011001000
192	010111	192	000011001001
256	0110111	256	000001011011
320	00110110	320	000000110011
384	00110111	384	000000110100
448	01100100	448	000000110101
512	01100101	512	000000110110
576	01101000	576	000000110111
640	01100111	640	000000101010
704	011001100	704	000000101011
768	011001101	768	000000101100
832	011010010	832	000000101101
896	011010011	896	000000111010
960	011010100	960	000000111011
1024	011010101	1024	000000111100
1088	011010110	1088	000000111101
1152	011010111	1152	000000111110
1216	011011000	1216	000000111111
1280	011011001	1280	000000101010
1344	011011010	1344	000000101011
1408	011011011	1408	000000101100
1472	010011000	1472	000000101101
1536	010011001	1536	000000101101
1600	010011010	1600	000000101101
1664	011000	1664	000000110010
1728	010011011	1728	000000110011
EOL	000000000001	EOL	000000000001

Note — It is recognized that machines exist which accommodate larger paper widths whilst maintaining the standard horizontal resolution. This option has been provided for by the addition of the Make-up code set defined as follows:

Table 2.2 - MHC Make-Up Code Table

Run length (black and white)	Make-up codes
1792	00000001000
1856	00000001100
1920	00000001101
1984	00000010010
2048	00000010011
2112	00000010100
2176	00000010101
2240	00000010110
2304	00000010111
2368	00000011100
2432	00000011101
2496	00000011110
2560	00000011111

Table 2.3 - MHC Extended Make-Up Code Table

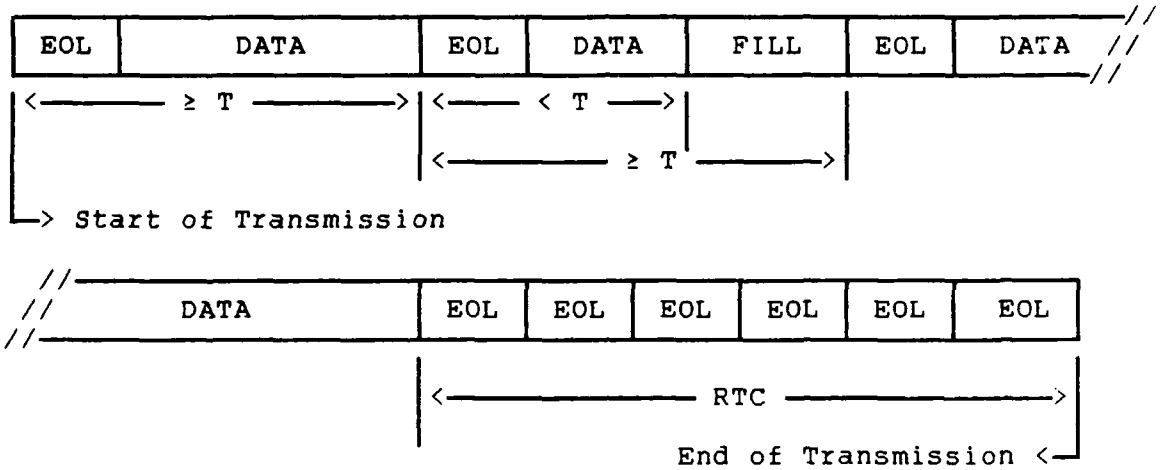
The format of the data stream in a Group 3 MHC transmission is presented in Figure 2.5. Each scan line is encoded individually and is separated from the other scan lines in the document with EOL's. Each coded scan line begins with a white run length code to ensure color synchronization at the receiver; if the actual scan line begins with a black run, a zero white run length code is inserted at the beginning of the coded scan line. Fill bits are inserted when the coded scan line is shorter than the minimum scan line transmission length T (in this study, T = 48 bits).

The two-dimensional run-length coding process, also known as Modified READ coding (MRC), compresses every Kth line in a document with MHC coding and the next (K - 1) lines with variable length code words derived from Table 2.4. The terms a_0, a_1, and a_2 in Table 2.4 refer to the positions of the reference changing element [1] and the next two changing elements, respectively, along the coding line; the terms b_1 and b_2 refer to the first and second changing elements on the reference line located to the right of a_0. The various coding modes associated with the MRC algorithm were selected so that the correlation between vertically adjacent pels was exploited. Figure 2.6 is a flow diagram which illustrates the coding process employed in the MRC algorithm; for a more detailed description of the mode selection process, see reference 4.

The format of a Group 3 MRC transmission is presented in Figure 2.7; this format is only slightly different from that employed in Group 3 MHC transmissions. As with the MHC format,

---

[1] A changing element is defined as a pel whose color is different from the previous pel along the same scan line.



EOL - End of line code - 000000000001

DATA - Coded scan line data

FILL - Transmission pause - variable length string of 0's

RTC - Return to control (End of message) code

T - Minimum scan line transmission length

Figure 2.5 - MHC Document Transmission Format

Two-dimensional code table

Mode	Elements to be coded		Notation	Code word
Pass	b_1, b_2		P	0001
Horizontal	a_0a_1, a_1a_2		H	001 + M(a_0a_1) + M(a_1a_2) (see Note)
Vertical	a_1 just under b_1	$a_1b_1 = 0$	V(0)	1
	a_1 to the right of b_1	$a_1b_1 = 1$	$V_R(1)$	011
		$a_1b_1 = 2$	$V_R(2)$	000011
		$a_1b_1 = 3$	$V_R(3)$	0000011
	a_1 to the left of b_1	$a_1b_1 = 1$	$V_L(1)$	010
		$a_1b_1 = 2$	$V_L(2)$	000010
		$a_1b_1 = 3$	$V_L(3)$	0000010
Extension	2-D (extensions) 1-D (extensions)			0000001xxx 000000001xxx (see Note 2)

Note 1 — Code M( ) of the horizontal mode represents the code words in Tables 1/T.4 and 2/T.4.

Note 2 — It is suggested the uncompressed mode is recognized as an optional extension of the two-dimensional coding scheme for Group 3 apparatus. The bit assignment for the xxx bits is 111 for the uncompressed mode of operation whose code table is given in Table 4/T.4.

Note 3 — Further study is needed to define other unspecified xxx bit assignments and their use for any further extensions.

Note 4 — If the suggested uncompressed mode is used on a line designated to be one-dimensionally coded, the coder must not switch into the uncompressed mode following any code word ending in the sequence 000. This is because any code word ending in 000 followed by a switching code 000000001 will be mistaken for an end-of-line code.

Uncompressed mode code words

Entrance code to uncompressed mode	On one-dimensionally coded line: 000000001111 On two-dimensionally coded line: 0000001111	
	Image pattern	*Code word*
Uncompressed mode code	1 01 001 0001 00001 00000	1 01 001 0001 00001 000001
Exist from uncompressed mode code	0 00 000 0000	0000001T 00000001T 000000001T 0000000001T 00000000001T

T denotes a tag bit which tells the colour of the next run (black = 1, white = 0).

Table 2.4 - MRC Two-Dimensional Code Table

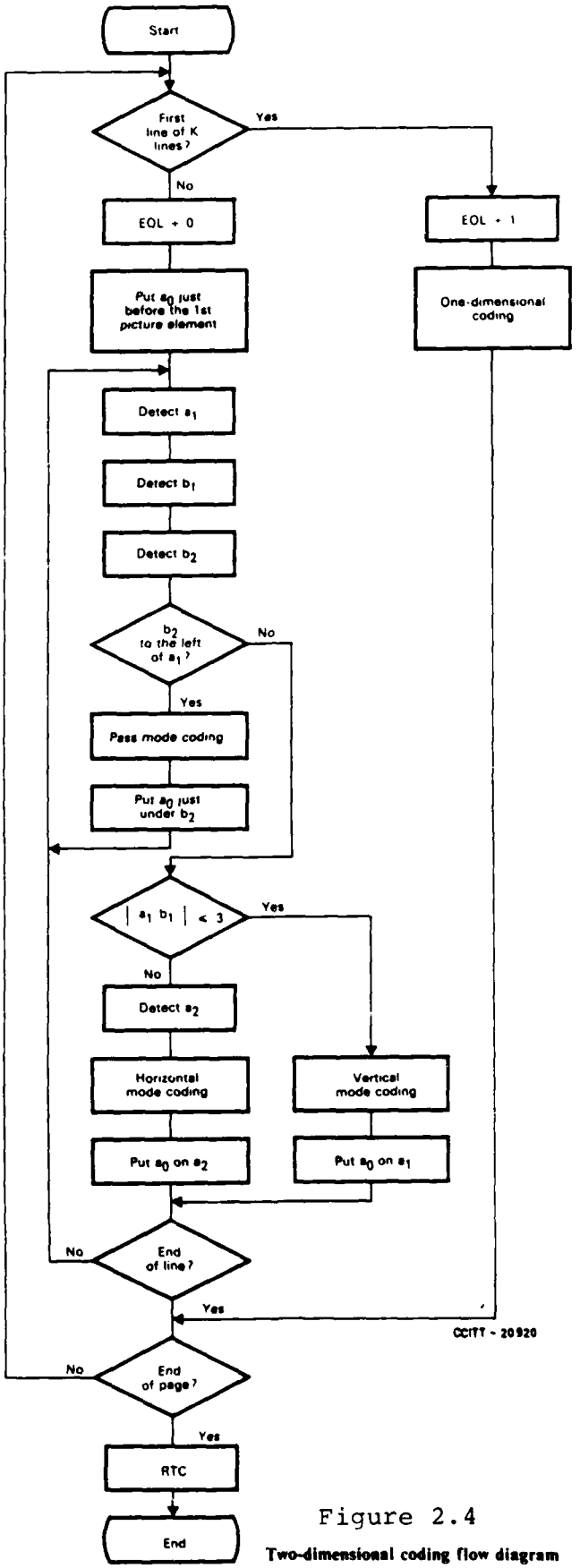
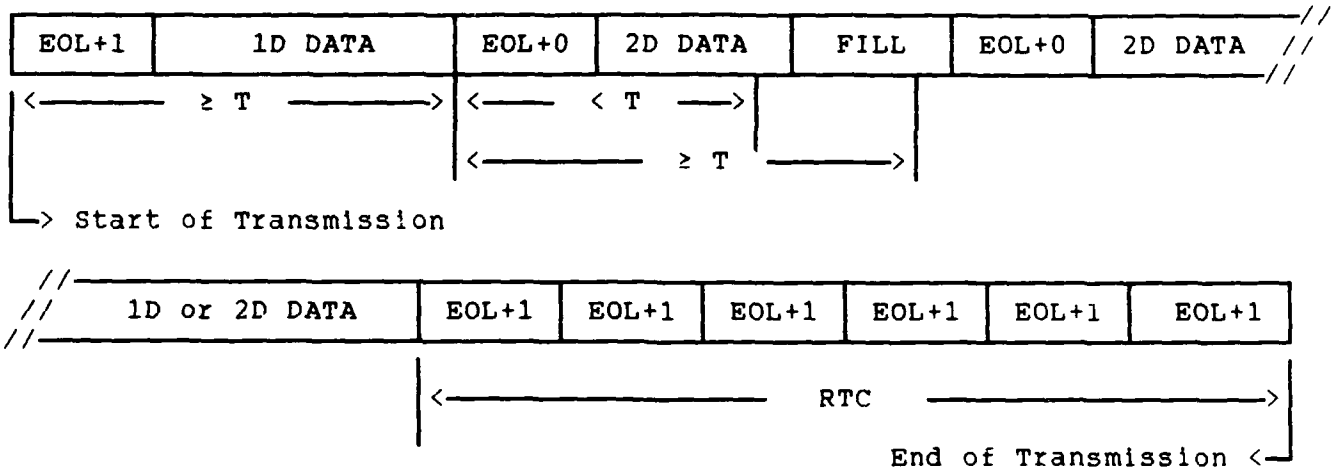


Figure 2.4

Two-dimensional coding flow diagram



EOL+t - End of line code - 000000000001 + Tag bit (1D=1, 2D=0)

DATA - Coded scan line data

FILL - Transmission pause - variable length string of 0's

RTC - Return to control (End of message) code

T - Minimum scan line transmission length

Figure 2.7 - MRC Document Transmission Format

each scan line is encoded individually and is separated from the other scan lines with EOL's; however, in addition to the 12-bit EOL code, a tag bit is added so that the receiver knows whether the scan line is 1D or 2D encoded. As before, fill bits are added so as to maintain the minimum scan line transmission length T.

2.3.2 DES Encryption Algorithm with 1-Bit Cipher Feedback

Figure 2.8 (ref. 8) is a functional block diagram of the DES encryption/decryption algorithm in the K-bit cipher feedback (CFB) mode; for secure Group 3 transmissions, K = 1. The encryptor is applied after the Group 3 encoding step (as in Figure 2.1) and before the coded data is sent through the transmission channel; the decryptor is applied just after the data is received from the transmission channel and just before the Group 3 decoding step. The plain text in and plain text out blocks in Figure 2.8 represent the coded data stream of the Group 3 transmission.

The encryption process is initiated by inserting a 64-bit key variable into the DES encryption module, either manually (i.e. keyboard, thumbwheel switches, etc.) or with an electronic key variable loader (ref. 5). This key variable consists of 56 randomly (or pseudorandomly) generated bits and 8 parity check bits, which are employed to ensure that the key variable is properly loaded. The principal function of the key variable is to set up the key schedule used in the encryption iterations; it can also be employed to create the 48-bit Initializing Vector

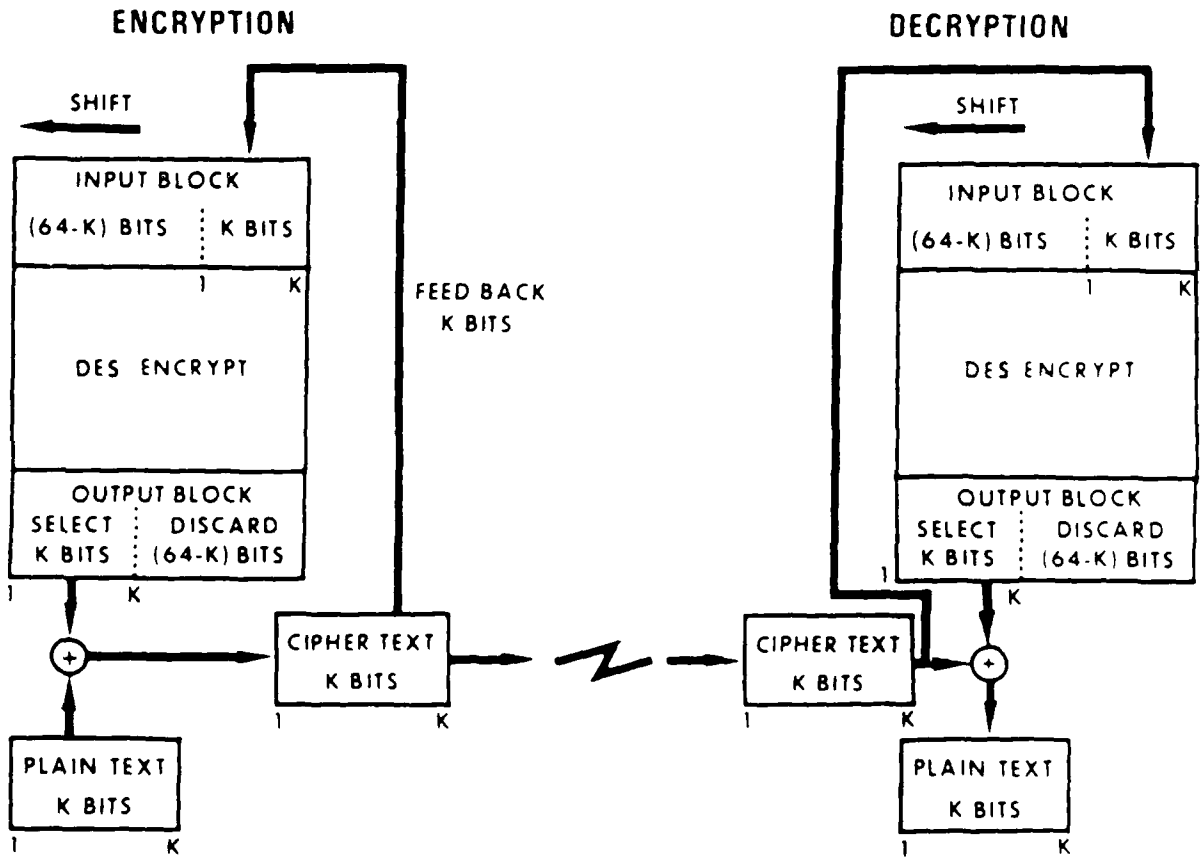


Figure 2.6 - DES Algorithm in the K-bit CFB Mode

(IV) that is loaded into the least significant bits of the DES input block at the beginning of the encryption and decryption steps.

The DES encryption algorithm, which is employed in both the encryption and decryption processes, consists of a series of bit matrix permutations and exclusive-OR operations as described in FIPS publication 46 (ref. 7). The DES encryption module takes a 64-bit input block (initially the 48-bit IV, right-justified, and 16 0's) and produces a 64-bit output block of encrypted data. In the 1-bit CFB mode, only the most significant bit of the DES output block is employed in the encryption/decryption process.

In the encryptor, the most significant bit of the DES output block is exclusive-ORed (XORed) with one bit from the coded data stream to produce a cipher bit; this cipher bit is loaded into both the enciphered data stream and the least significant bit of the DES input block, which is left-shifted to accommodate the cipher feedback bit. The most significant bit of the DES input block is discarded, as are the remaining 63 bits of the DES output block. This process continues for each bit in the coded data stream until the entire document is encoded and enciphered.

In the decryptor, the algorithm employed is basically identical to the one used in the encryption process, where the same key variable is employed to set up the key schedule and generate the IV; the one exception is that the cipher bit is fed forward (with an initial 1 bit delay) rather than back, as in the encryption process (see Figure 2.8).

2.3.3 Error Signal Algorithms

Two error signal types were selected for evaluation in this study. The first, a single burst error signal, is characterized by a random pattern of error bursts; an error burst consists of a group of 8 bits, 4 error bits alternating with 4 correct bits. Figure 2.9 illustrates the structure of the single burst error pattern. For each transmission segment of L bits, there is an error burst located N_i bits from the beginning of the segment. In this study, the random nature of the error burst pattern was approximated with a pseudorandom number generator known as the method of congruence (ref. 3); the pseudorandom numbers N_i, i=1,2,... in Figure 2.9 were obtained from the equation

$$N_{i+1} = aN_i + c \pmod{M} \quad ,$$

where c and M are prime number constants. The choice of M was determined by the integer arithmetic computational capacity of the computer employed (M = 62144 for the HP1000); a and c were selected so as to maximize the randomness of the error burst pattern (a = 6237, c = 5439).

The second type of error signal evaluated was the double burst signal, the structure of which is illustrated in Figure 2.10. A variation of the single error burst signal, this signal is characterized by groups of two error bursts, called disturbances, distributed randomly. For each transmission segment of L bits, a disturbance is located N_i bits from the beginning of the segment. The distance between the two bursts within a disturbance d_i varies from 2 to 17 bits in a periodic sawtooth pattern; that is, the spacing between the bursts

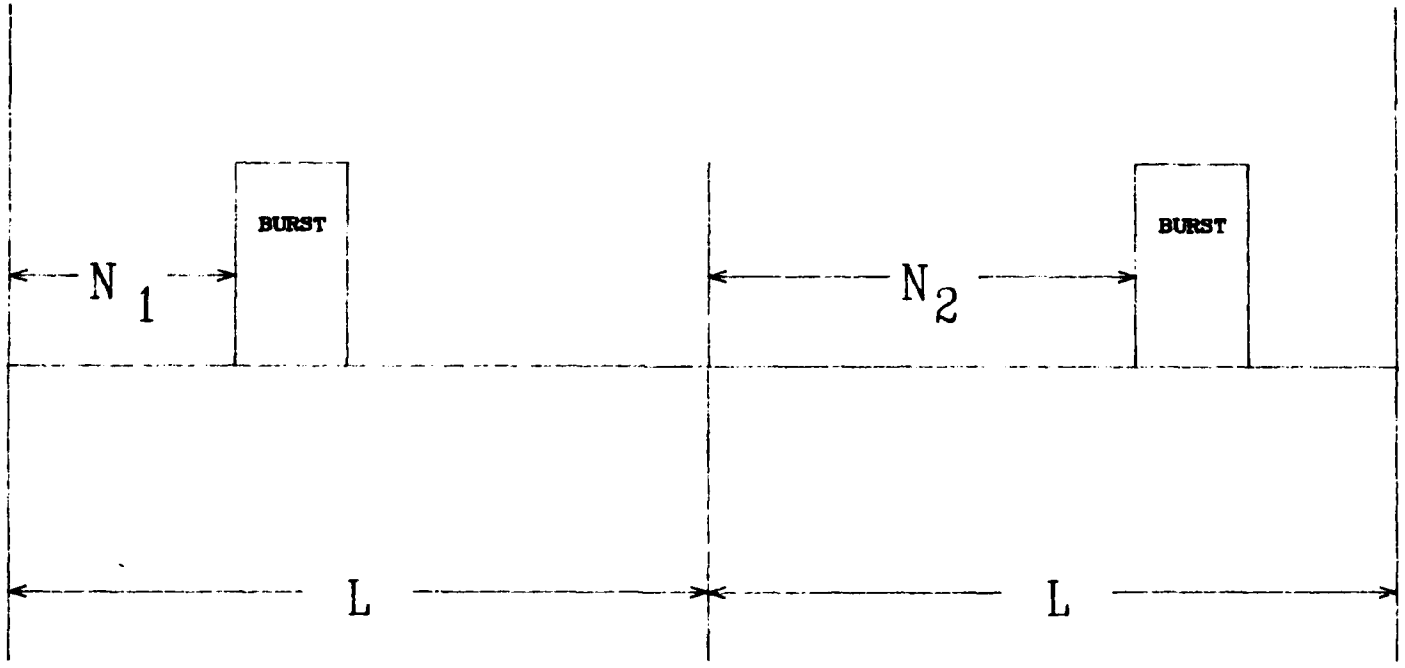


Figure 2.9 – Single Burst Error Pattern Structure

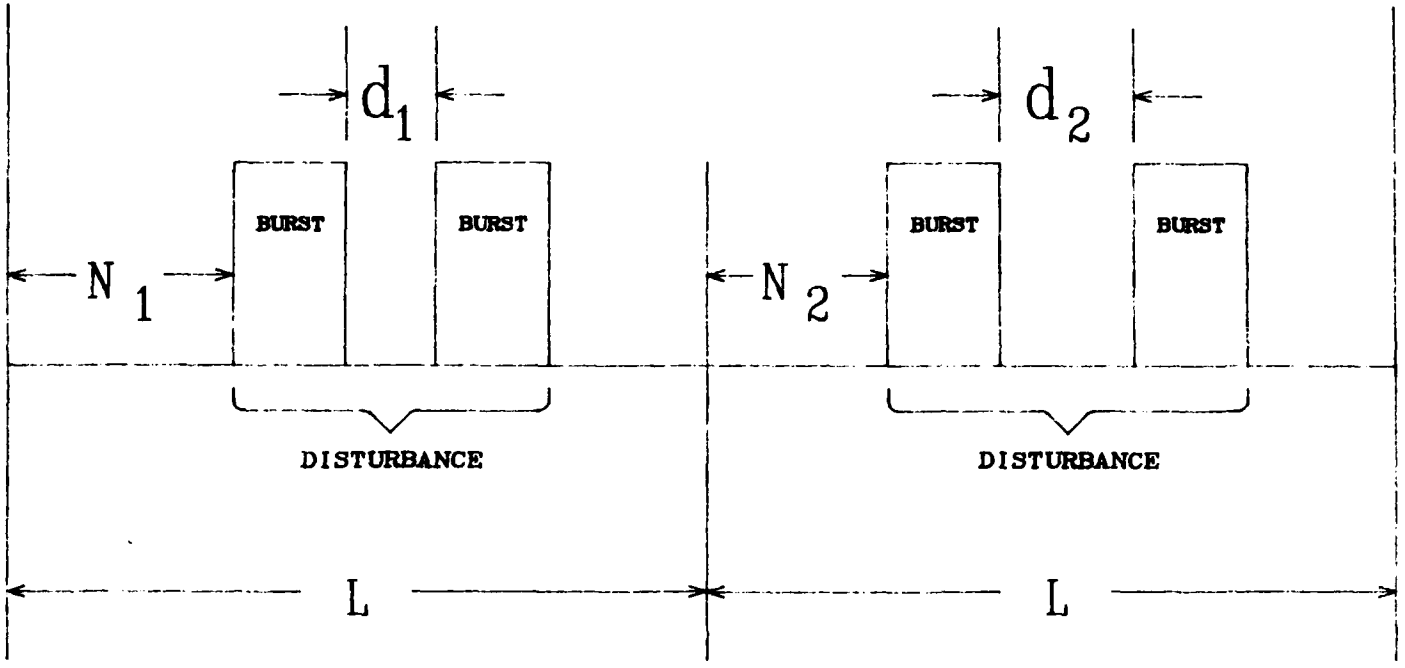


Figure 2.10 – Double Burst Error Pattern Structure

increases linearly for 16 disturbances and then repeats. The same pseudorandom number generator employed to approximate the random nature of the single burst error signal was employed for the double burst error signal.

3.0 RESULTS

3.1 Error Sensitivity Statistics

Table 3.1 is a summary of the error sensitivity results obtained from the 48 simulation runs performed in this study. Sixteen simulations were performed for each of the three test documents (CCITT documents #1, #5, #7), including all combinations of the following parameters:

2 compression algorithms - MHC, MRC

2 Bit Error Rates - 4×10^{-3}, 1×10^{-3}

2 Error Signal Types - Single Burst, Double Burst

2 Error Signal Conditions - With, without encryption

The error sensitivity factor (ESF) in Table 3.1 is defined as the ratio between the number of error bits in the output file and the number of error bits inserted to simulate transmission link errors. This ratio represents the average disturbance to the output image caused by a single transmission error.

The bit error rate (BER) in Table 3.1 is defined as the ratio between error bits and total bits in the transmitted bit stream. The two bit rates employed in this study were selected based upon the bit rates employed in a previous study (ref. 3); the BER of 4×10^{-3} was selected directly from the previous study and the BER of 1×10^{-3} was selected after the initial simulations indicated that the first BER was relatively high.

Table 3.1 - Error Sensitivity Results - Page 1 of 3

CCITT Image Number	Compression Algorithm	Error Type	Bit Error Rate	Number of Error Bits Inserted	Number of Error Bits After Decryption	Number of Error Bits in Output	Error Sensitivity Factor
1	MHC	Single Burst Only	$4x10^{-3}$	1148	---	29905	26.05
			$1x10^{-3}$	288	---	4472	15.53
		Single Burst + Decrypt	$4x10^{-3}$	1148	10906	34057	29.67
			$1x10^{-3}$	288	2736	5318	18.47
		Double Burst Only	$4x10^{-3}$	1144	---	11850	10.36
			$1x10^{-3}$	288	---	3018	10.48
		Double Burst + Decrypt	$4x10^{-3}$	1144	5846	13065	11.42
			$1x10^{-3}$	288	1446	3061	10.63
	MRC	Single Burst Only	$4x10^{-3}$	916	---	55173	60.23
			$1x10^{-3}$	228	---	20120	88.25
		Single Burst + Decrypt	$4x10^{-3}$	916	8702	62159	67.86
			$1x10^{-3}$	228	2166	20175	88.49
		Double Burst Only	$4x10^{-3}$	912	---	40989	44.94
			$1x10^{-3}$	232	---	8113	34.97
		Double Burst + Decrypt	$4x10^{-3}$	912	4650	41275	45.26
			$1x10^{-3}$	232	1174	7342	31.65

Table 3.1 - Error Sensitivity Results - Page 2 of 3

CCITT Image Number	Compression Algorithm	Error Type	Bit Error Rate	Number of Error Bits Inserted	Number of Error Bits After Decryption	Number of Error Bits in Output	Error Sensitivity Factor
5	MHC	Single Burst Only	$4x10^{-3}$	1896	---	55286	29.16
			$1x10^{-3}$	476	---	9488	19.93
		Single Burst + Decrypt	$4x10^{-3}$	1896	18012	63610	33.55
			$1x10^{-3}$	476	4522	10405	21.86
		Double Burst Only	$4x10^{-3}$	1904	---	21838	11.47
			$1x10^{-3}$	480	---	3442	7.17
		Double Burst + Decrypt	$4x10^{-3}$	1904	9732	22595	11.87
			$1x10^{-3}$	480	2443	3794	7.90
	MRC	Single Burst Only	$4x10^{-3}$	1320	---	124093	94.01
			$1x10^{-3}$	328	---	34514	105.23
		Single Burst + Decrypt	$4x10^{-3}$	1320	12540	133093	100.83
			$1x10^{-3}$	328	3116	35315	107.67
		Double Burst Only	$4x10^{-3}$	1320	---	67308	50.99
			$1x10^{-3}$	328	---	19416	59.20
		Double Burst + Decrypt	$4x10^{-3}$	1320	6722	70494	53.40
			$1x10^{-3}$	328	1659	20761	63.30

Table 3.1 - Error Sensitivity Results - Page 3 of 3

CCITT Image Number	Compression Algorithm	Error Type	Bit Error Rate	Number of Error Bits Inserted	Number of Error Bits After Decryption	Number of Error Bits in Output	Error Sensitivity Factor
7	MHC	Single Burst Only	$4x10^{-3}$	3268	---	93385	28.58
			$1x10^{-3}$	820	---	20328	24.79
		Single Burst + Decrypt	$4x10^{-3}$	3268	31046	106959	32.73
			$1x10^{-3}$	820	7790	22663	27.64
		Double Burst Only	$4x10^{-3}$	3272	---	43180	13.20
			$1x10^{-3}$	816	---	10933	13.40
		Double Burst + Decrypt	$4x10^{-3}$	3272	16724	48936	14.96
			$1x10^{-3}$	816	4145	11977	14.68
	MRC	Single Burst Only	$4x10^{-3}$	2504	---	222924	89.03
			$1x10^{-3}$	624	---	57282	91.80
		Single Burst + Decrypt	$4x10^{-3}$	2504	23788	231791	92.57
			$1x10^{-3}$	624	5928	62720	10.58
		Double Burst Only	$4x10^{-3}$	2504	---	120148	47.98
			$1x10^{-3}$	624	---	30073	48.19
		Double Burst + Decrypt	$4x10^{-3}$	2504	12794	128445	51.30
			$1x10^{-3}$	624	3182	32739	52.47

These bit rates were calculated as follows:

Single Burst:

$$BER = \frac{\text{\# error bits/burst}}{\text{\# bits/segment length L}}$$

$$BER = \frac{4}{(L = 1024)} = .00391 = 4 \times 10^{-3}$$

$$BER = \frac{4}{(L = 4096)} = .00098 = 1 \times 10^{-3}$$

Double Burst:

$$BER = \frac{\text{\# error bits/disturbance}}{\text{\# bits/segment length L}}$$

$$BER = \frac{8}{(L = 2048)} = .00391 = 4 \times 10^{-3}$$

$$BER = \frac{8}{(L = 8192)} = .00098 = 1 \times 10^{-3}$$

Note that the segment lengths used to generate the single and double burst error patterns were selected so that the same bit error rates were used for both error signal types.

The results presented in Table 3.1 indicate that the error signal type has a significant effect on the number of errors caused by the decryption process. The number of errors inserted (to simulate transmission link errors) is the same (within $\pm$ 4 bits) for both single and double burst error signals, yet the decryption of a file containing single burst errors causes $\approx$10:1 expansion in the number of errors produced, while the decryption of a file corrupted with double burst errors causes only $\approx$5:1

expansion. This indicates that the number of error bits within a burst (or disturbance) has less of an effect on the number of errors produced by the decryption process than the number of error groups [2] present (For a given BER, there are twice as many single burst error groups inserted as there are double burst disturbance groups.).

In terms of error sensitivity, the runs in which single burst error signals were employed had higher ESF values than those runs in which double burst error signals were employed (e.g. 26.05 vs. 10.36 for Document #1, MHC, single burst only, BER = 4×10^{-3}). The simulations in which the MHC compression algorithm was employed had lower ESF values than the simulations in which the MRC compression was employed (e.g. 33.55 vs. 100.83 for document #5, single burst + decrypt, BER = 4×10^{-3}), indicating that the two-dimensional MRC algorithm is more sensitive to transmission errors than the one-dimensional MHC algorithm.

The effect of the decryption process on the error sensitivity of Group 3 facsimile appears, at first, to be significant. For single burst error signals, the decryption process causes the number of errors in the coded data stream to expand by $\approx$10:1, while for double burst error signals it causes the number of errors in the coded data stream to expand by $\approx$5:1. However, upon decoding, the number of errors produced in the

---

[2] An error group is defined as an error burst for single burst errors and as an error disturbance for double burst errors.

output image is small in comparison to these ratios. The largest increase in ESF value obtained in this study was 18.9% (18.47 vs. 15.53, document #1, MHC, single burst, BER = 1×10^{-3}); in one instance, the ESF value actually decreased by 9.5% (31.65 vs. 34.97, document #1, MRC, double burst, BER = 1×10^{-3}) despite the $\approx$5:1 expansion in the number of error bits in the coded data stream.

Table 3.2 summarizes the percent increases in error sensitivity due to the decryption process, averaged over the three test documents, for each of the eight combinations of compression algorithm, error signal type, and bit error rate analyzed in this study. These results indicate that, while the MHC compression algorithm is less sensitive to transmission errors than the MRC algorithm, the effect of the decryption process on the error sensitivity of the MHC algorithm is greater than its effect on that of the MRC algorithm. In other words, on the average, the decryption process caused a greater increase in the ESF values of those simulation runs in which the MHC was employed than in those runs in which the MRC algorithm was employed.

3.2 Output Images

Table 3.3 is a list of the images included in this report in order to illustrate the effects of encryption on the error sensitivity of Group 3 facsimile. Document #1, the English

Table 3.2 - Percent Change in Error Sensitivity

Compression Algorithm	Error Type	Bit Error Rate	Average Percent Increase in ESF (Error Sensitivity)
MHC	Single Burst	4x10-3	14.5
		1x10-3	13.4
	Double Burst	4x10-3	13.3
		1x10-3	7.1
MRC	Single Burst	4x10-3	8.0
		1x10-3	4.0
	Double Burst	4x10-3	4.1
		1x10-3	2.1

Table 3.3 - List of Output Images

CCITT Image Number	Compression Algorithm	Error Type	Bit Error Rate	Figure Number
1	MHC	Single Burst Only	4x10-3	3.2
			1x10-3	3.3
		Single Burst + Decrypt	4x10-3	3.4
			1x10-3	3.5
		Double Burst Only	4x10-3	3.6
			1x10-3	3.7
		Double Burst + Decrypt	4x10-3	3.8
			1x10-3	3.9
	MRC	Single Burst Only	4x10-3	3.10
			1x10-3	3.11
		Single Burst + Decrypt	4x10-3	3.12
			1x10-3	3.13
		Double Burst Only	4x10-3	3.14
			1x10-3	3.15
		Double Burst + Decrypt	4x10-3	3.16
			1x10-3	3.17

letter, was selected for illustration purposes; it was not necessary to include all three test documents, as the visual degradation caused by the error signals is relatively consistent over the three. As stated earlier, the decryption of a corrupted coded data stream results in $\approx$10:1 expansion in the number of errors in the coded data stream for single burst errors and $\approx$5:1 expansion for double burst errors. The number of errors that appear in the decoded output error image, however, does not reflect this significant error propagation; in fact, the increase in the number of errors in the output image resulting from the decryption process did not exceed 20% in the simulation runs performed. Averaged over the three test documents, the increase in the number of errors occurring in the output image ranged from 2% to 15%, depending on the parameters employed.

Figure 3.1 represents the decrypted and decoded document in the case where no errors are introduced by the transmission link; it is an exact reproduction of the input document (Note that the images shown in Figures 3.1 through 3.17 are slightly smaller sections of the full sized images.). Figures 3.2 through 3.17 are the output images resulting from the 16 simulation runs performed with document #1 as the test image. As with the ESF values, the simulation runs in which the MHC compression algorithm was employed were much less sensitive to transmission errors in terms of output image quality than those in which the MRC algorithm was employed (e.g. compare Figures 3.4, MHC, and 3.12, MRC, single burst + decrypt, BER = 4×10^{-3}).

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH 25 8 ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC 18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.1

Registered in England: No. 2068
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH25 8ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.2

THE SLEREXE COMPANY LIMITED

SAPORS LANE . BOOLE . DORSET . BH 25 8 ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.3

Registered in England: No. 2068
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH25 8ER

TELEPHONE BOOLE (0945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.4

Registered in England: No. 6555
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE · BOOLE · DORSET · BH 25 8 ER

TELEPHONE BOOLE (945 13) 51617 · TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.5

Registered in England: No. 2038
Registered Office: 60 Vicarage Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE . BOOLE . DORSET . BH25 8ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/FAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.6

Registered in England: No. 2008
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH25 8ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.7

Registered in England: No. 2038
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE . BOOLE . DORSET . BH25 8ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/FAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.8

Registered in England: No. 2038
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH 25 8 ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.9

Registered in England: No. 2068
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEEVE COMPANY LIMITED

[illegible] . [illegible] [illegible] - [illegible]

TELEPHONE BOOLE (945 13) 51617 · TELEX 123456

Our Ref. 330/PJC/PAC 18th January, 1972.

Dr P N Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogue electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

P.J.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.10

THE SLEREXE COMPANY LIMITED

SAPORS LANE · BOOLE · DORSET · BH25 8ER

TELEPHONE BOOLE (945 13) 51617 · TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronized with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.11

Registered in England: No. 2008
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEEVE COMPANY LIMITED

SABORE LANE . [illegible] . [illegible] . [illegible]

TELEPHONE BOOLE (945 13) 51617 TELEX 123456

Our Ref. 350/PJC/TAC 16th January 1972.

Dr P N Cundall
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

[illegible] transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogue electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result a facsimile copy of the subject document is produced.

Probably you have used one this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.12

Registered in England No 9029
Registered Office [illegible]

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH25 8ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/FAC 18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.13

Registered in England: No. 8008
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SIEMENS COMPANY LIMITED

SAMUEL LANE . WIMBORNE . DORSET . BH21 8ER

TELEPHONE WIMBORNE (0202) 51617 - TELEX 123456

Our Ref. 350/PJC/PAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.14

Registered in England: No. 0088
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH 25 8 ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC

18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.15

Registered in England: No. 2068
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEEKEX COMPANY LIMITED

SAMONS LANE . WOOLF . DORSET . BH25 8ED

TELEPHONE WOOLF (0425 13) 21617 - TELEX 123456

Our Ref. 350/PJC/EAC. 18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading,
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.16

Registered in England: No. 0038
Registered Office: 60 Vicars Lane, Ilford, Essex.

THE SLEREXE COMPANY LIMITED

SAPORS LANE - BOOLE - DORSET - BH25 8ER

TELEPHONE BOOLE (945 13) 51617 - TELEX 123456

Our Ref. 350/PJC/EAC 18th January, 1972.

Dr. P.N. Cundall,
Mining Surveys Ltd.,
Holroyd Road,
Reading.
Berks.

Dear Pete,

Permit me to introduce you to the facility of facsimile transmission.

In facsimile a photocell is caused to perform a raster scan over the subject copy. The variations of print density on the document cause the photocell to generate an analogous electrical video signal. This signal is used to modulate a carrier, which is transmitted to a remote destination over a radio or cable communications link.

At the remote terminal, demodulation reconstructs the video signal, which is used to modulate the density of print produced by a printing device. This device is scanning in a raster scan synchronised with that at the transmitting terminal. As a result, a facsimile copy of the subject document is produced.

Probably you have uses for this facility in your organisation.

Yours sincerely,

Phil.

P.J. CROSS
Group Leader - Facsimile Research

FIGURE 3.17

Registered in England: No. 2068
Registered Office: 60 Vicars Lane, Ilford, Essex.

In comparing the output image quality between simulations in which single burst error signals were employed and simulations in which double burst error signals were employed, the differences in visual image quality were again significant. Figures 3.10 (MRC, single burst only, BER = 4×10^{-3}) and 3.14 (MRC, double burst only, BER = 4×10^{-3}) show that the single burst error signal has more of an effect on the output image quality than the double burst error signal; Figure 3.14 is somewhat legible whereas Figure 3.10 is almost completely degraded. This result supports with the conclusion arrived at in the statistical analysis that the number of error groups in an error signal has a greater effect on error sensitivity than the number of errors within the error groups.

The effect of the decryption process on the error sensitivity is small in terms of ESF value compared to the effects due to compression algorithm, error signal structure, and BER; this is even more true in terms of visual image quality. In comparing Figures 3.10 and 3.12 (MRC, single burst, BER = 4×10^{-3} there are obvious differences (e.g. the first sentence of the letter), and the decryption does cause some additional image degradation, but the legibility of both documents is virtually non-existent. A comparison of Figures 3.2 and 3.4 (MHC, single burst, BER = 4×10^{-3}), the case in which the increase in the ESF value due to the decryption process was greatest (18.9%), shows that the legibility of the output image is only slightly reduced.

The reduction in the bit error rate from 4×10^{-3} to 1×10^{-3} had the effect of, in general, increasing the ESF value for the simulations in which the MRC compression algorithm was employed and decreasing it for the simulations in which the MHC algorithm was employed. Of course, the lower BER increased the output image quality as compared to the higher BER (compare Figures 3.12 and 3.13, MRC, single burst + decrypt). The output image quality of the simulation runs in which the MHC compression algorithm and the lower BER were employed was excellent both with and without encryption (see Figures 3.3, 3.5, 3.7, and 3.9), indicating that secure Group 3 transmissions can be successful at this error rate. In fact, the output image quality of the simulations in which the MRC algorithm was employed was only slightly less than acceptable in the presence of single burst errors at the lower BER and was only slightly degraded in the presence of double burst errors.

4.0 CONCLUSIONS AND RECOMMENDATIONS

In analyzing the results presented in Section 3.0, several conclusions were drawn concerning the effect of transmission errors on the error sensitivity of secure Group 3 facsimile. These conclusions, in turn, led to the formulation of a number of recommendations as to which direction future work in this area should be directed.

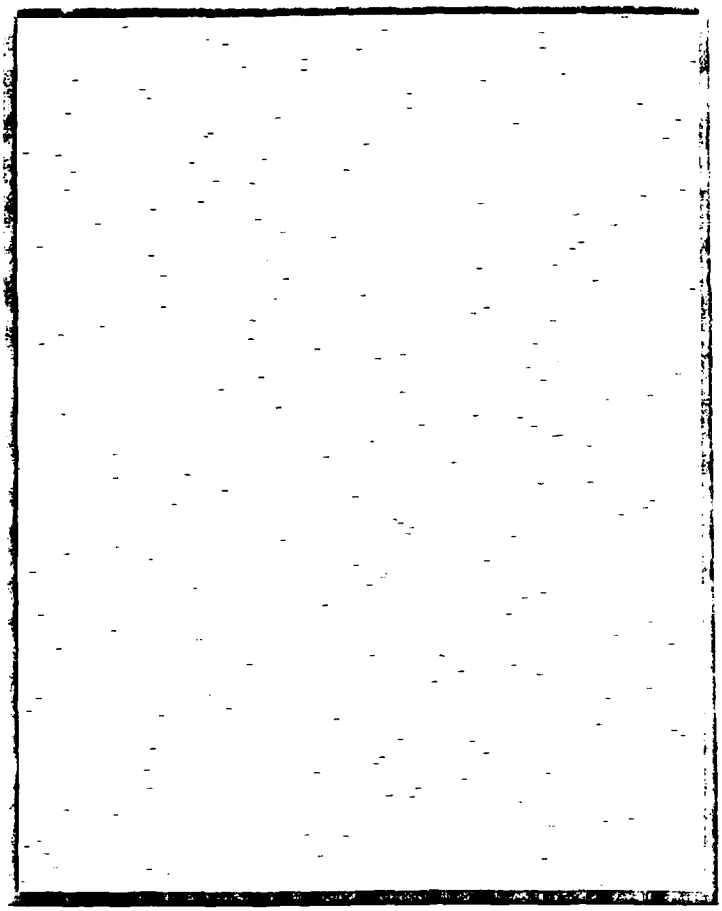
4.1 Conclusions

1. The DES encryption process does cause a moderate increase in the sensitivity of Group 3 facsimile to data link errors, but not in proportion to the number of error bits it introduces into the encoded data stream of a Group 3 facsimile transmission.
2. The output image quality produced by simulations in which encryption was employed was only slightly more degraded than that of simulations in which it was not, indicating that the large number of errors introduced by the decryption of an encoded data stream are not manifested in the output image.
3. The number of errors within an error group has less of an effect on error sensitivity than the number of error groups in the error signal. This accounts for the fact that the single burst error signals had a greater effect on error sensitivity than the double

burst error signals; it also accounts for the fact that the large number of error bits introduced into the encoded data stream by the decryption process did not cause a correspondingly large number of errors in the output image. The error groups are expanded by 5 to 10:1, but they remain in the same basic area in the encoded data stream and thus cause only a modest expansion in the number of errors in the decoded output image. Figure 4.1 contains an example of an encoded data stream with data link errors before encryption, and Figure 4.2 is the same data stream after decryption; the error bits, while significantly greater in number, remain localized.

4. The Modified Huffman coding algorithm appears to be less sensitive to transmission errors than the Modified READ algorithm; in applications where output image quality is more important than compression, the MHC algorithm should be employed.

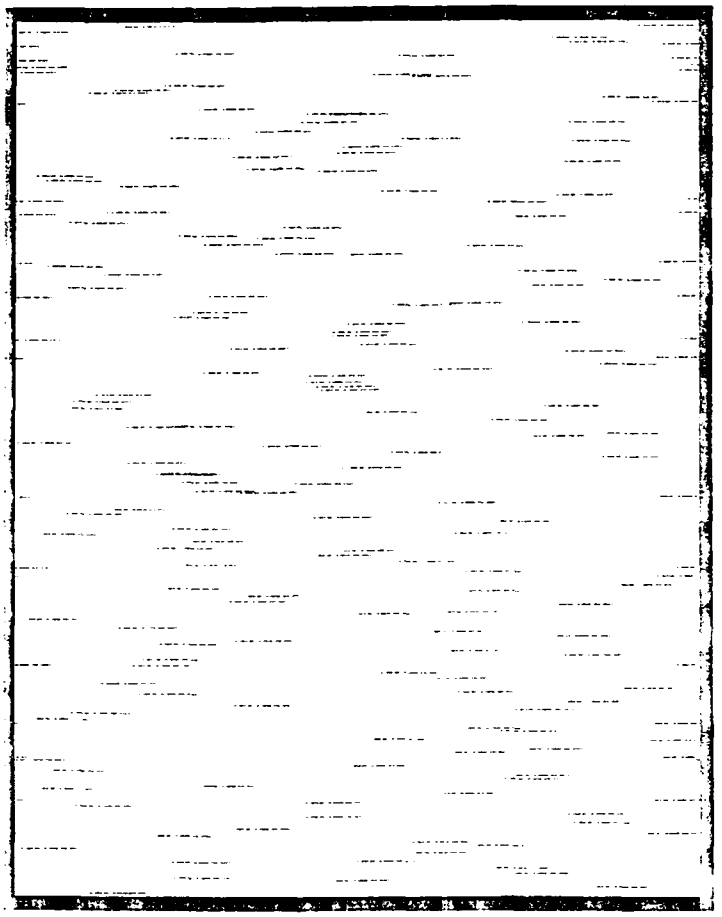
5. The bit error rate of 1×10^{-3} appears to be near the upper limit, in terms of output image quality, of the MRC compression algorithm's sensitivity toward error rate. The legibility of the output images produced by the simulations performed with this BER and the MRC algorithm is fair; the legibility produced in the simulations in which the BER of 4×10^{-3} and the MRC algorithm were employed was very poor.



Black - Error Bit

White - Correct Bit

Figure 4.1 - Encoded Data Stream with Single Burst Errors



Black - Error Bit

White - Correct Bit

Figure 4.2 - Encoded Data Stream with Single Burst Errors and Errors Due to Decryption

4.2 Recommendations for Further Study

1. Additional error signal types, including random bit errors and random-burst error combinations, should be investigated to determine their effects on the error sensitivity of secure Group 3 facsimile transmissions.

2. The effects of various error control techniques on secure Group 3 facsimile should be explored; although these techniques reduce the number of errors introduced by the data link, they also introduce new error patterns that could have a significant effect on the decryption process.

REFERENCES

1. "Development of a Computer Program for Measuring the Compression and Error Sensitivity of Facsimile Coding Techniques", Delta Information Systems, P. O. Number DCA-100-79-M-0105, August 10, 1979.

2. "Measurement of Compression Factor and Error Sensitivity Factor of Facsimile Coding Submitted to the CCITT by Great Britain and Germany", Delta Information Systems, P. O. Number DCA-100-79-M-0209, October, 1979.

3. "Sensitivity of Digital Facsimile Coding Techniques to Simulated Burst Errors", Delta Information Systems, P. O. Number DCA-100-80-M-0005, June, 1980.

4. "Standardization of Group 3 Facsimile Apparatus for Document Transmission", CCITT Recommendation T.4, October, 1984.

5. "Telecommunciations: General Security Requirements for Equipment Using the Data Encryption Standard", FED-STD-1027, April 14, 1982.

6. "Telecommunications: Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment", FED-STD-1028, Pre-publication copy.

7. "Data Encryption Standard", FIPS Publication 46, January 15, 1977.

8. "DES Modes of Operation", FIPS Publication 81, December 2, 1980.