Frame Based Symmetric Key Cryptography

Uttam Kr. Mondal
Dept. of CSE & IT,College of Engg. & Management, Kolaghat , Midnapur(W.B), India.
Email: uttam_ku_82@yahoo.co.in
Satyendra Nath Mandal
Dept. of IT, Kalyani Govt. Engg. College,Kalyani, Nadia(W.B),India
Email: satyen_kgec@rediffmail.com
J. PalChoudhury
Dept. of IT, Kalyani Govt. Engg. College,Kalyani, Nadia(W.B),India.
Email: jnpc193@yahoo.com
J.K.Mandal
Dept. of CSE, University of Kalyani, Nadia(W.B),India
Email: jkm.cse@gmail.com

ABSTRACT

There are huge numbers of algorithms available in symmetry key block cipher. All these algorithms have been used either complicated keys to produce cipher text from plain text or a complicated algorithms for it. The level of security of all algorithms is dependent on either number of iterations or length of keys. In this paper, a symmetry key block cipher algorithm has been proposed to encrypt plain text into cipher text or vice versa using a frame set. A comparative study have been made with RSA, DES, IDEA, BAM and other algorithms with Chi-square value, frequency distribution, bit ratio to check the security level of proposed algorithm. Finally, a comparison has been made for time complexity for encryption of plain text and decryption from cipher text with the well-known existing algorithms.

Keywords - **cryptography, plain text, cipher text, symmetric key algorithm, chi - square and frequency distributions.**

Date of Submission: April 24, 2010 Revised: September 06, 2010 Date of Acceptance: October 10, 2010

1. Introduction

Cryptography is the study of transmitting secret messages securely from one party to another. To accomplish this task, the original text, called plain text, is “translated” into an encrypted version called cipher text, which is sent to the intended recipient. The recipient decrypts the text to obtain the original message. The model of secret key system, first proposed by Shannon ([1]) is shown in figure 1.

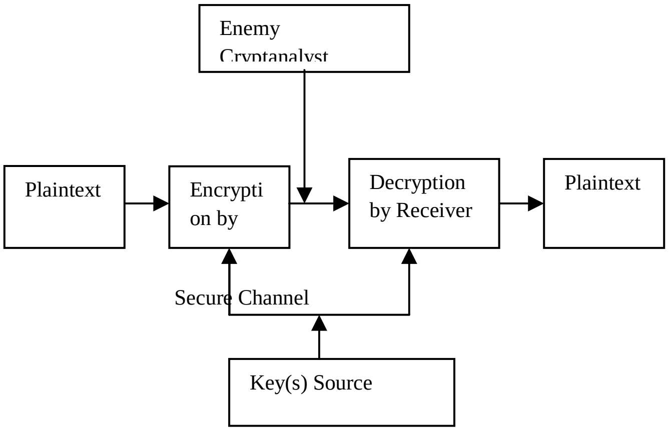


Fig 1:The model of secret key system proposed by Shannon

Many algorithms have been developed to providing security of information but each of them having some merits and demerits. No single algorithm is sufficient for this purpose. As a result researchers are working in the field of cryptography to remove the deficiency and finding better solution.

In this paper, an effort has been made to develop a new block cipher algorithms using a set of 16 frames where each frame is 4X4 matrix. Each frame is capable to store 16 characters and finally, all extended ASCII characters have been stored in this frame set. The algorithm has been written into two steps. In first step, the plaintext has been broken into number of block eight characters. Each character from each block has been converted into bit stream and placed in the frame set. After placing all characters, new bit stream for each character of the block has been calculated using frame number, row number and column number. In second step, new block has been made by placing each bit from each character bits stream from its corresponding position into all positions according the characters position of the block i.e. bits from zero position of all characters in the block will form bits stream of zero position character of cipher block, bits from one position of all characters in the block will form bits stream of one position character of the cipher block, so on.

Section 2 of the paper deals with the background theory of cryptography technique. The proposed technique has been depicted in section 3. Experimental results are given in section 4. Securities level testing for the proposed algorithm is made in section 5. Conclusions are drawn in section 6. References are given at end.

2. Theory

2.1 Cryptographic Techniques

Cryptography, a word with Greek origins, means “secret writing”. However, we use the term to the science and art of transforming messages to make them secure and immune to attacks. The original message, before transformed, is called plaintext. After the message is transformed, it is called cipher text. The process of encoding plain text messages into cipher text messages is called encryption. The reverse process of transforming cipher text messages back to plain text is called decryption. If the same key is used for encryption and decryption, we call the mechanism as Symmetric Key Cryptography. Cipher text = encrypt (plaintext, key),Plaintext = decrypt (cipher text, key). If two different keys are used in a cryptographic mechanism, wherein one key is used for encryption, and another, different keys are used for decryption; we call the mechanism as Asymmetric Key Cryptography.

2.2 Security Level Testing for a Cryptographic Algorithm

To ensure the security level of a cryptographic algorithm many effects have been made. Among of them avalanche, bit ratio, non-homogeneity, frequency distribution, time complexity are frequently used in practice. The avalanche effect means a small change in plain text (or key) should create a significant change in cipher text. The bit ratio effect means the changes the bit values from same position between plain text and cipher text. The non-homogeneity test is a technique to test non-homogeneity of the source and encrypted file. Actually, the chi-square value on degree of freedom of any file indicates the homogeneity of this file. In the frequency distribution graph of source and encrypted file by proposed algorithm will be displayed. If the characters in the encrypted file are evenly distributed, it will make the cryptanalysis more difficult. The time complexity indicates how efficiently the proposed algorithm will encrypt the plain text and decrypt from encrypted text.

3. Proposed Algorithms (FBSKC)

3.1 Method of Encryption

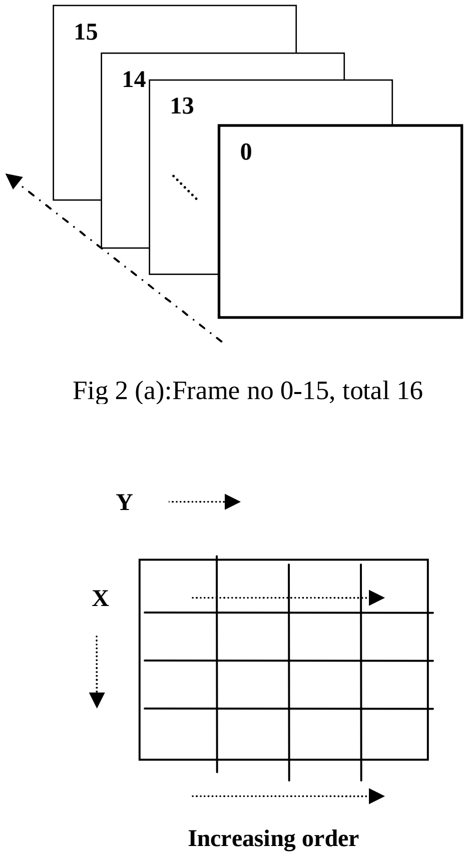


Fig 2 (a):Frame no 0-15, total 16

Fig 2 (b): A single frame

Fig 2: Structure of reference frame

The key of the algorithms are based on the reference frame given in figure 2. A single frame consists of 16 characters, i.e. then total number of frame is 16 (256/16) required for representing extend ASCII set.

Algorithms:

Step 1: Represent each character of plain text by another character which is equivalent a number, generated from reference. frame model (figure 1). Then, the substitute character is represented by the bit sequence (x,y,frame no).

Step 2: Grouping the modified plain text into blocks of eight characters. If modified test is not properly divided by eight then blank characters will be padded with last block .

Step 3: Convert each block into equivalent bit streams.

Step 4: Cipher block has been computed by placing position of bits of each character corresponding each position i.e. all bits from zero positions from eight characters have been placed consecutively to form cipher character in position zero of cipher block The i^{th} character (0<=i<=7) of taken input group is represented by the set of 8 bits , substituted each position by i^{th} bit of 1st , 2nd , 3rd,4th , 5th , 6th, 7th, 8th character of input block respectively.

Step 5: Repeat steps 2 to 4 until all characters of plain text become converted into cipher text.

3.2 Method of Decryption

Step 1: Grouping the cipher text into blocks of eight characters.

Step 2: Convert each block into equivalent bit streams

Step 3: Decrypted block has been computed by placing position of bits of each character corresponding each position i.e. all bits from zero positions from eight characters have been placed consecutively to form decrypted character in position zero of decrypted block. The i^{th} character (0<=i<=7) of taken cipher characters group is represented by the set of 8 bits , substituted each position by $(7-i)^{th}$ bit of 1st , 2nd , 3rd,4th , 5th , 6th, 7th, 8th character of cipher block respectively.

Step 4: Represent each character of modified text (using step3) by another character which is equivalent a number, generated from reference frame model of figure 2. Finally, decrypted text is getting by the following calculation. Let, the modified bit sequence of a character is (x, y, frame no). Then, ASCII value of decrypt character is **(16*(frameno+1)+x*4+y).**

3.2 Example

Let, we have an input file with following contains: Cryptography & Network Security.

3.2.1 Encryption

Applying encryption algorithm we get following Cipher text:

Character	ASCII value	(x,y,frame no)	Replaced Char	Generated bit stream using step 4	Cipher chararcter
C	67	0,3,3	00110011	10000110	†
r	114	0,2,6	00100110	11111001	ù
y	121	2,1,6	10010110	01111111	
p	112	0,0,6	00000110	00000000	
t	116	1,0,6	01000110	10100110	¦
o	1111	3,3,5	11110101	11000111	Ç
g	103	1,3,5	01110101	00001110	
r	114	0,2,6	00100110	00100100	$
…	…	…	…	…	…

Table 1: Encrypted characters

3.2.2 Decryption

Applying decryption algorithm we will get plain text back.

Charact	ASCII value	Generated bit stream using	**(16*frameno + x*4+y)**	Decrypted
†	10000110	00110011	16*(3+1)+0+3=67	C
Ù	11111001	00100110	114	r
	01111111	10010110	121	y
	00000000	00000110	112	p
¦	10100110	01000110	116	t
Ç	11000111	11110101	1111	o
	00001110	01110101	103	g
$	00100100	00100110	114	r
…	…	…	…	…

Table 2: Decrypted character

4. Experimental Result

4.1 Plain text

```
The best part of beauty is that which no
picture can express.An error doesn't

become a mistake until you refuse to
correct it.Freedom rings wherever

opinions clash.Sincerity and truth are
the basis of every virtue.Ability is

poor manâ€™s wealth.
```

4.2 Cipher Text

```
|_ï_&

¥@§X{_"_
_ñ_~_:@,_RÞ_Ä@_ˆ €û_±“ƒk±N _5_

 ü_w_dP__O´ò_tºJ

_
hû_‘y“_·Lï_Õr¹$ÿ_õ_õÀqažaý_ÝH%ˆºE÷_',Ó¶³L~_.T
:_y†ß_Y^ÉH¶KÙ_ ‡N_ý_û_Ù_ø_Ö)ï_jéÊ„Zÿ_Tä

÷_û_jº±ñ·@ï_Í[_6§Xû_ªA‘)Ã<¾___¬_·Hî_¢@*_×(û_z
«__Ò-}_T)q_ rù_šE<„æ_û_«_Pê·Èû€³82²µjëPkª£°ß
ð_€_hX€€€€€ _€
```

5. Security Level Testing

5.1 Frequency Distribution Test

In the frequency distribution graph of source and encrypted file by proposed algorithm will be displayed. If the characters in the encrypted file are evenly distributed, it will make the cryptanalysis more difficult. In fig 3 is showing the frequency distribution graph of different algorithms where blue color graph representing the frequency distribution for plain text and saffron color is representing the frequency distribution for encrypted text of different algorithms. From above figure 3, it is cleared that the frequency distribution of our cipher text is better than other existing algorithm showing above(figure 3.1 to figure 3.4)

5.2 Non-Homogeneity Test

The non-homogeneity test is a technique to test non-homogeneity of the source and encrypted file. Actually, the chi-square value on degree of freedom of any file indicates the homogeneity of this file. If the computed chi-square value is much more than the actual chi-square value, the file is non-homogeneous. The high chi-square value proved that source and corresponding encrypted files are heterogeneous [7]. The degree of freedom is found to be 256. The chi-square value and degree of freedom of different algorithms have been presented in table3, where C, D are used for represent Chi-square value, degree of freedom respectively.

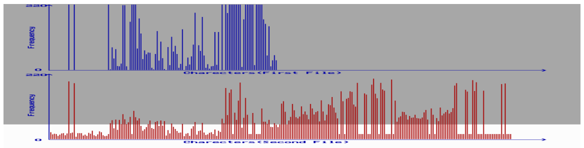


Fig 3.1 Frequency Distribution of BAM.

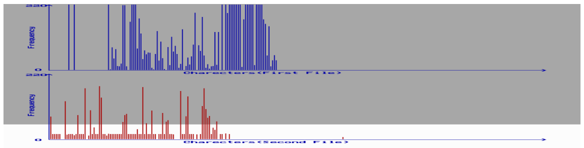


Fig 3.2 Frequency Distribution of RSA.

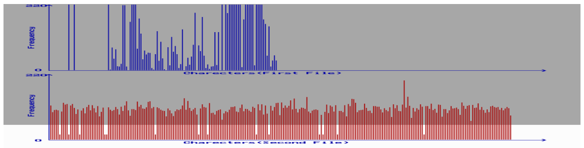


Fig 3.3: Frequency Distribution of DES.

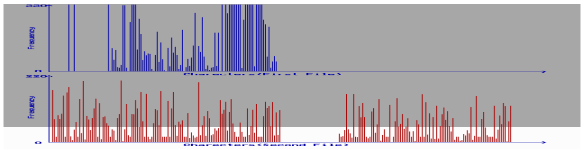


Fig 3.4: Frequency Distribution of IDEA

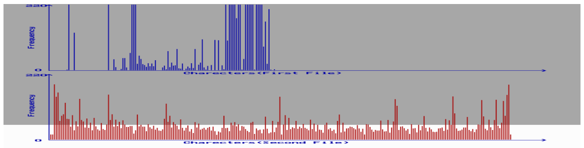


Fig 3.5: Frequency Distribution of FBSKC

Fig 3 : Frequency Distribution of different algorithms

Sl. No.	Source files with size	FBSKC	BAM	RSA	IDEA	Tripple DES
1	file01.txt 18 kb	C-34085 D-256	C-31474 D-245	C-35302 D-101	C=3199 D=117	C-33451 D-256
2	file02.txt 22 kb	C-41686 D-256	C-38754 D-249	C-42708 D-109	C=6862 D=158	C-40683 D-256
3	file03.txt 17 kb	C-31758 D-256	C-29708 D-249	C-33121 D-113	C=15554 D=185	C-31032 D-256
4	file04.txt 16 kb	C-29119 D-256	C-27028 D-238	C-30054 D-98	C=51206 D=208	C-28536 D-256
5	file05.txt 9 kb	C-15339 D-252	C-14366 D-231	C-15927 D-94	C=24482 D=291	C-14934 D-256
6	file06.txt 26 kb	C-49052 D-256	C-46068 D-254	C-50301 D-110	C=28835 D=197	C-47750 D-256
7	file07.txt 9 kb	C-16871 D-255	C-15899 D-236	C-17404 D-93	C=18951 D=194	C-16477 D-256
8	file08.txt 13 kb	C-24354 D-256	C-23447 D-233	C-25116 D-100	C=28782 D=202	C-23850 D-256
9	file09.txt 27 kb	C-50861 D-256	C-47057 D-255	C-52748 D-114	C=41655 D=205	C-49522 D-256
10	file10.txt 10 kb	C-18816 D-256	C-18034 D-236	C-19608 D-113	C=49291 D=207	C-18316 D-256

Table 3: Chi – Square and degree of freedom

From above table3, it is cleared that the produce chi-square value and degree of freedom of our proposed algorithm are better than other existing algorithms.

5.3 Bit-Ratio Test

The bit ratio effect means the changes the bit values from same position between plain text and cipher text. The bit-ratio can be determined as:

Bit-ratio (in %) = {(Total number of bits changed in the file after encryption) ÷ (Total number of bits present in the file)} × 100.

File Name	File Size (kb)	Bit Ratio			
		BAM	RSA	DES	FBSKC
File 01	1.752 kb	46.08	45.34	47.57	48.19
File 02	3.676 kb	45.15	44.85	46.43	45.72
File 03	8.356 kb	46.81	45.09	47.36	46.23
File 04	27.452 kb	45.01	44.87	46.78	47.99
File 05	13.020 kb	44.97	43.90	43.97	48.87
File 06	15.448 kb	45.21	44.98	44.76	46.13
File 07	10.152 kb	46.12	45.56	45.24	49.56
File 08	15.400 kb	44.97	44.06	45.93	47.41
File 09	22.380 kb	43.63	42.06	42.76	46.82
File 10	26.208 kb	43.87	43.20	42.78	48.19

Table 4: Bit-Ratio comparison

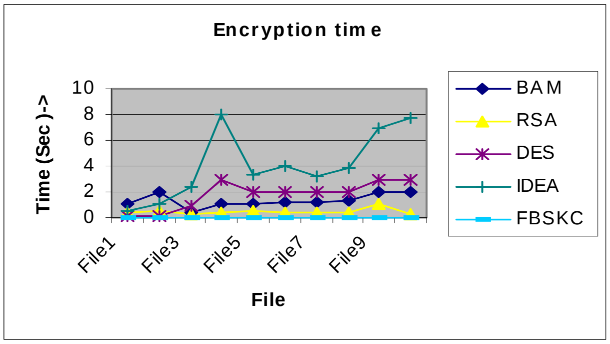
Table 4 is representing the average bit-ratio of our proposed algorithm is better than the other existing algorithms which is graphically presented in graph 1.

[redacted]

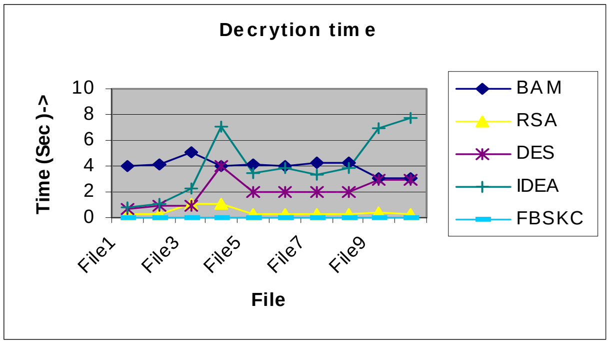
Graph 1: bit-ratio comparison

5.4 Encryption and Decryption time Comparison

The time complexity indicates how efficiently the proposed algorithm will encrypt the plain text and decrypt from encrypted text. If the time complexity is much lower than time complexity on the same file of other existing algorithms, the proposed algorithm is better than existing algorithms.



Graph 2: encryption time



Graph 3: decryption time

Table 5 representing the required time for both encryption and decryption of different algorithms and it is cleared that our algorithm takes less time respect to other algorithms. Graph 2 and graph 3 are graphically presenting encryption and decryption time respectively for different algorithms.

5.4 Vulnerability

Time required to use a brute force approach, which simply involves trying every possible key until an intelligent translation of the cipher text into plain text is obtained. On average, half of all possible key must be tried to achieve success. Table 6 shows how much time is involved for various key spaces.

Key size (bits)	No. of alternate Keys	Time required at 1 encryption / μs	Time required at 10^6 encryption/ μs
56	2^{56}=7.2*10^{16}	2^{55} μs=1142 years	10.01 hours
64	**2^{64}=1.8*10^{19}**	**2^{63} μs=2.9*10^{5} yrs**	**106.75 days**
128	**2^{128}=3.4*10^{38}**	**2^{127} μs=5.3*10^{24} yrs**	**5. 3*10^{18} yrs**

Table 6: Average time required for exhaustive key search Analysis

Results are shown for two binary sizes. The 56-bits key size is used with the DES (Data Encryption Standard) algorithm, 64-bit key size is used for our proposed algorithm. For each key size the results are shown assuming that it takes 1 μs perform a single decryption, which is a reasonable order of magnitude for today's machine. Within the use of massively parallel organizations of microprocessors, it may be possible to achieve processing rates may orders of magnitude greater. The final column of the table 6 considers the result for a system that can process a 1(one) millions keys per microsecond. As the key size increases, the complexity of exhaustive search becomes infeasible to crack encryption directly.Algorithm with key of 56 bits (DES) is taken 1142 years and our proposed algorithm needs 2.9*10^5 years (of considering 64 bits) to search appropriate key to crack encryption. As one can see at this performance level (considering above Table 6), DES can no longer be considered computationally secure compare to our proposed algorithm. Even, increasing reference frame size (of 128 bits, 160 bits or 168 bits etc) we able to achieve more security level comparing with other available existing standard algorithms.

5. Conclusion and Future Work

On the basis of the observed experimental results, it can be said that 'FBSKC 'is extremely efficient and a sufficiently strong cryptographic algorithm that provides a superior level of security.

- From the comparison with other cryptosystems based on Chi –Square values & Degree of Freedom, it has been proved that 'FBSKC ' always provides a much higher value of degree of freedom compared to RSA, BAM, IDEA and DES. It can therefore safely be said that the cipher text using the proposed algorithm is completely heterogeneous with respect to the original text. A degree of freedom value of 256 ensures the maximum variety of characters in the cipher text which ensures its strength against an attack.

- From the comparison based on Encryption and Decryption time, it has been well proved that in the ground of time complexity, use of 'FBSKC' is always far more advantageous.
- The comparison of Frequency Distribution also speaks the encrypted character evenly distributed from 0 to 255. So, it has been made more difficult for attacker to recover plain text from cipher text.

Above all, the proposed algorithm is a simple, straight-forward but intrinsically strong and compact approach to cryptography using the essence of genetic operations. It provides the same or sometimes even better level of security using minimal time complexity. The most striking feature of 'FBSKC' is that it is a far faster cryptographic algorithm than DES and it provides maximum heterogeneous possible in the cipher text in the most cost-efficient manner. A comparative study and security level will be verified in future with other well known algorithms.

REFERENCES

[1] C.E. Shannan, "Communication Theory of Security System", Bell, System Technical Journal , vol 28,pp.656-715,1949.

[2] Nalini. N and G. Raghavendra Rao," A New Encryption and Decryption Algorithm Combining the Features of Genetic Algorithms(GA) and Cryptography"

[3] H. Feistel ," Cryptography and Computer Privacy", Scientific American Vol. 228 ,no. 5,pp 15-23,1973.

[4] Wiliam Stallings, Cryptography and Network ,3rd edition ,Penntice Hall,ISBN 0-13-111502-2, 2003.

[5] Behrouz A. Forouzan," Cryptography & Network Security", Tata McGraw Hill, ISBN 13-978-0-07-066046-5.

[6] Schneier B," Applied Cryptography - Protocols, Algorithms and Source Code in C", Second Edition ,New York, John Wiley & Sons, 1996,ISBN 0-471-11709-9.

[7] A.M. Goon, M. K.Gupta, B. Dasgupta " Fundamental of Statistics", vol 1, World Press Ltd.

[8] Uttam Kr. Mondal , Satyendra Nath Mandal , J. PalChoudhury, J.K.Mandal, "A New Approach to Cryptography", *International Conference Systematics, Cybernatics & Informatics (ICSCI 2008)* , Page pp. 294-297, Jan. 07-10,2009.

Authors Biography

Uttam Kr. Mondal, has received his Bachelor of Engineering (B.E) degree in Information Technology in 2004 and Master of Technology (M.Tech) in Information Technology in 2006 from University of Calcutta, India. He has now working as a Lecturer in department of Computer Science & Engineering and Information Technology in College of Engg. & Management,Kalaghat,West Bengal, India. His research areas include cryptography & Network Security, Audio signal authentication. He has 8 publications in National and International conference proceedings

Satyendra Nath Mandal has received his B.Tech & M.Tech in Computer Science & Engineering from university of Calcutta, West Bengal India. He is now working as a lecturer in department of Information Technology at Kalyani Govt. Engg. College , Kalyani , Nadia, West Bengal, India. His field of research areas includes cryptography & network Security, fuzzy logic, Artificial Neural Network, Genetic Algorithm etc. He has about 25 research papers in national and International conferences. His three research papers have been published in International journal.

J. Paul Choudhury(Jagannibas Paul Choudhury) completed Bachelor of Electronics and Tele-Communication Engineering(Hons) from Jadavpur University, Kolkata M. Tech in Electronics and Electrical Engineering under the specialization of Control and Automation Engineering from Indian Institute of Technology, Kharagpur and. thereafter completed PhD(Engg) from Jadavpur University, Kolkata. At present Dr. Paul Choudhury is with Information Technology

Department, Kalyani Government Engineering College, Dt Nadia, West Bengal, India, and he has 60 publications in National and International Journals and in Conference Proceedings. His field of interest is Soft Computing, Data Base, Object Oriented Methodology, etc

Joytsna Kumar Mandal, M.Tech. (Computer Science, University of Calcutta) , Ph.D. (Engg., Jadavpur University) in the field of Data Compression and Error Correction technique, Professor in Computer Science and Engineering,University of Kalyani,India.Life Member of Computer Society of India since 1992. Dean, faculty of Engineering, Teaching & Management,working in the field of Network Security ,Staganography,Remote sensing & GIS application,Image Processing .23 years of teaching and research experiences.7 Scholars awarded Ph.D.;1 Scholars submitted Ph.D., 5 scholars are registered for Ph.D and 3 scholars are enrolled for Ph.D..Total number of publications 138.

Source	BAM		RSA		DES		IDEA		FBSKC	
	Enc	Dec	Enc.	Dec.	Enc.	Dec	Enc.	Dec.	Enc	Dec
File1	1.02	4.01	0.45	0.33	0.12	0.67	0.578	0.750	0.037	0.037
File2	2.03	4.10	0.50	0.33	0.10	1.0	1.125	1.127	0.039	0.039
File3	0.42	5.04	0.32	1.01	1.0	1.0	2.343	2.328	0.036	0.036
File4	1.02	4.03	0.39	1.01	3.0	4.0	7.984	7.094	0.036	0.035
File5	1.12	4.15	0.54	0.21	2.0	2.0	3.328	3.409	0.031	0.030
File6	1.25	4.04	0.34	0.33	2.0	2.0	3.985	3.909	0.042	0.056
File7	1.14	4.21	0.42	0.22	2.0	2.0	3.265	3.268	0.045	0.031
File8	1.32	4.23	0.34	0.32	2.0	2.0	3.890	3.891	0.033	0.033
File9	2.00	3.09	1.01	0.34	3.0	3.0	6.937	6.937	0.043	0.057
File10	2.01	3.03	0.21	0.22	3.0	3.0	7.750	7.794	0.032	0.031

Table 5: Time Complexity Analysis