# A Survey On SecureImage Encryption Technique Using Blowfish And Chaos

Romani Patel[1],Krunal Panchal[2]

[1]*Research Scholar, Information Technology, L.J Institute Of Engineering And Technology, Ahmedabad, Gujarat, India*
[2]*Assistant Professor,Information Technology, L.J Institute Of Engineering And Technology, Ahmedabad, Gujarat, India*

**Abstract**

*This paper focuses mainly on the different kinds of image encryption and decryption techniques. In addition focuses on image encryption techniques. In this paper mainly focuses on two techniques like that blowfish and chaos. Security has always been a great concern whenever there is communication between sender and receiver. To overcome the issues of security breaches many cryptographic algorithms are used like: aes, des, blowfish etc. Blowfish algorithm more compact and more secure compare to aes algorithm. Blowfish algorithm is a symmetric block cipher with a 64-bit block size and variable key lengths from 32 bits up to a maximum of 448 bits.*Blowfish is a secret symmetric key that has only a single key, used both for encryption and decryption. The algorithm consists of two parts. One is a Key-expansion part and one more is a data-encryption part. The blowfish uses a large number of sub keys. Blowfish is one of the fastest block ciphers in general use, expect when changing keys. *chaos has been widely used for image encryption for its different features. There are many chaos based encryption techniques. Chaos used for expand diffusion & confusion in image. Most of the proposed discrete chaotic cryptographic approaches are based on stream or block cipher schemes. Chaos-based cryptography is a promising and emerging field that offers a large variety of techniques particularly suitable for applications such as image encryption. The fundamental characteristics of chaotic systems are closely related to the properties of a strong cryptosystem. Most research on chaos-based encryption does not concentrate on the aspect of encryption modes of operation.*

**Keywords**- *Image Encryption, Image Decryption, Blowfish, Chaos, AES*

## INTRODUCTION

Cryptography is an essential part for the Information Security System(ISS). Cryptography algorithms are always in use because of security issues. Performance of cryptography algorithm is totally dependent on the size of file. Currently size of data is exponentially increasing, so cryptography algorithms take more time to execute.The Cryptography used today gives many essential techniques for protecting data and securing information. Mainly two types of cryptography are known : Asymmetric key cryptography and Symmetric key cryptography[1].

### 1.1 BLOWFISH

Blowfish is a secret symmetric key that has only a single key, used both for encryption and decryption. And cipher based on blocks, which also uses Blowfish, based on a Feistel- Network. A Feistel iterates a specific function a certain number of times and each cycle is called a round. Blowfish has a round number of 16. In addition to the Feistel Network, Blowfish bases its action on 4 arrays like SBoxes, each box contain 256 independent keys [1].

The blowfish encryption algorithm consists of two major steps

1) Sub-key Generation

This process is key dependent. It involves generating two sub key arrays P and S-box. P is a 1-D array of size 18; each element is a 32-bit unsigned integer. S-box is a 4 x 256 substitution box (A lookup table) each entry is a 32-bitunsigned integer. They are both initialized with a constant string (Hexadecimal digits of ʌ).

The first step is to split the key into 32 bit segments and XOR them with their corresponding segments in the P array. If the key is shorter than 576 bits (32 x 18) then the key is cycled through starting from the beginning till all the elements of the P array are XORed.

Next, the all zero string is encrypted using the Blowfish algorithm, using the modified P-array from above, to get as output a new 64-bit encrypted block. Pi is then replaced with the first 32 bits of the output and Pi+1 with the next 32 bits. This process is repeated till all the elements in the P array are modified (i: 0 Í17) and the process is repeated for the S substitution box as well. The sub-keys are then ready for usage. This process has to be carried out once every time the key is changed.

S1,0, S1,1,..., S1,255;

S2,0, S2,1,..,, S2,255;

S3,0, S3,1,..., S3,255;

S4,0, S4,1,..,, S4,255;

In Blowfish, one P-Box (could be considered arrays) is present which contain 18 32-bit keys.

P1, P2, P3……., P17,P18;

Each input block is 64 bits long, while the key can be as long as 448bits. There is an irreversible function F( ) which is only One Way[1].

2) Encryption: Feistel network consisting of 16 rounds.

The input is a 64-bit data element, x.

Divide x into two 32-bit halves: xL, xR

- For i = 1 to 16:
- xL = xL XOR Pi
- xR = F(xL) XOR xR
- Swap xL and xR
- Next i
- Swap xL and xR (Undo the last swap.)
- xR = xR XOR P17
- xL = xL XOR P18
- Recombine xL and xR
- End

Decryption is exactly the same as encryption, except that P-Box[ P1, P2,..., P18 ] is used in the reverse order.

**Function F**:-Divide xL into four eight-bit quarters named as a, b, c, and d

F(xL) = ( ( S1, a + S2, b mod 232 ) XOR S3, c ) + S4, d mod 232

### 1.2 CHAOS

chaotic encryption methods are based on single discrete-time chaotic map, through pixel value substitution or pixel position permutation. Image cipher scheme based on single discrete-time chaotic system is fast in speed, but weak in key space and security. For pixel value substitution, the encrypted image can be deciphered after the attacker decrypt the image encryption matrix. And for pixel position permutation, the attacker can decipher the encrypted image through methods based on statistical analysis, since the color histogram stay unchangeable in the cipher process[2].

Chaos Encryption algorithm work on sequence based.

Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit sensitivity to initial condition and have random like behaviour. Mathematically one dimensional chaos map can be represented as:

$$Xp+1 = f(Xp),\ f: I \rightarrow I,\ Xo\ \varepsilon\ I,$$

Where f is a continuous map on the interval I = [0, 1].

With the following propriety:

Sensitive to initial condition. This sensitivity property is utilized for the keys of cryptosystems.

Topological transitivity which linked to the diffusion feature of cryptosystem.

Above two properties often used to construct stream cipher and block cipher in chaotic cryptography. Because the property of sensitivity of initial condition make the encryption very complicated. Sequence is also sensitive to control parameter[7]

For image encryption chaotic system can be represented

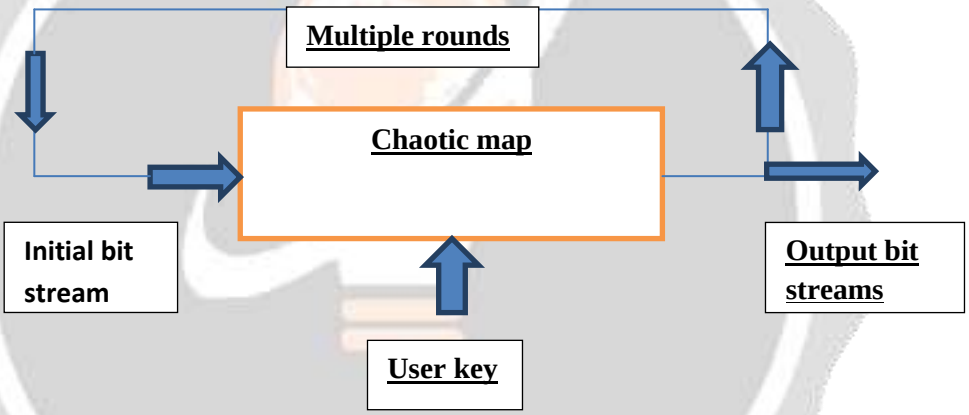


Fig 1 Chaos based encryption.[7]

In Fig 1.The initial value of chaotic map takes the original image as input sequence of bit provided by user mapped as control parameter. Output chaotic sequence produces the cipher image. Basic architecture of chaotic map small change in input bit stream produce a huge change in output bit stream after multiple round. Slight change of user key also produces totally different output sequence of bit stream[7].

## 2. RELATED WORK

**Novel Color Image Encryption Technique using Blowfish and Cross Chaos Map**

we have proposed a double encryption technique using Blowfish algorithm and Cross chaos map. These techniques have been chosen due to their resistance over the cryptanalysis attacks.Simulation and analysis results have shown that the BOLWFISH-CROSS-CHAOS is able to protect different types of images with a high level of security[3].

**Analysis of modified Blowfish Algorithm in different cases with various parameters**

The objective of this paper is to enhance and evaluate the Blowfish algorithm on the basis of different parameters like Encryption Quality, Correlation Coefficients, Key Sensitivity Test and Size of Output File. The 'f' function is modified by mixing the XOR and addition used in the original algorithm. Four cases are created and analyzed. The results of all the tests conducted on these cases lead to a common conclusion that the security of the modified algorithm with different cases makes the original Blowfish algorithm more compact and more secure than the earlier[4].

**Edge Based Block Wise Selective Fingerprint Image Encryption Using Chaos**

This paper proposes an efficient and lossless method for securing fingerprint images using edge based block wise selective encryption based on chaotic theory. In this proposed technique, fingerprint image is segmented into significant and non significant blocks and encryption is applied upon significant blocks which reduces the computational overhead and processing time as compared to full encryption techniques. Experimental results shows that edge based block wise selective encryption significantly reduces the time of encryption of fingerprint images as compared to full encryption method without any compromise in performance which suits real time applications. Experimental results also indicate that upon decryption data is completely recovered making the proposed scheme lossless in nature which suits the requirements of biometric pattern recognition. Further key sensitivity analysis shows that in order to obtain original image after decryption the correct combination of encryption keys is required[5].

**A New Chaos-Based Secure Image Encryption Scheme Using Multiple Substitution Boxes**

In this paper, confusion and diffusion phenomenon is presented for digital images. The proposed scheme provides a secure image encryption/decryption scheme using two chaotic maps and substitution boxes. In confusion process, the plaintext image is permuted row-wise and column-wise via two random sequences generated by Henon map. The pixel values diffusion is carried out by unimodel Skew tent map through XOR operation. Furthermore, in last step of the proposed scheme, image is divided into four blocks. To get a highly diffused ciphertext, four different Substitution Boxes (S-Boxes) are applied on each block. Initial conditions and control parameters of the Henon and Skew tent maps provide good security attributes.Simulation results show that the ciphertext histogram of the proposed scheme is almost flat. Further experimental results show that the proposed scheme is also resistant against various statistical and differential attacks[6].

**Image Encryption using Chaos Theory**

Chaos has been widely used for image encryption for its different features. Most of the proposed discrete chaotic cryptographic approaches are based on stream or block cipher schemes. If these two schemes are combined the security level is improved. Novel image encryption is proposed based on combination of pixel shuffling .Chaos is used for expand diffusion & confusion in image. We survey exiting work which uses different techniques for image encryption and analyse them with respect to various parameters.Results of our analyses indicate that the new scheme has a satisfactory security level with a low computational complexity, which renders it a good candidate for real-time secure image transmission applications.. So, it is a challenge for a research to design an encryption scheme which maintains good tradeoff among tunability, visual degradation, compression friendliness, format compliance, encryption ratio, speed, and cryptographic security[7].

**A Hybrid Algorithm for Enhanced Image Security Using Chaos and DNA theory**

An image encryption algorithm based on chaotic theory and Deoxyribonucleic acid (DNA) sequencing is proposed here. Initially, two chaotic sequences are generated from the logistic map function, one for image permutation and other for image diffusion. The two internal secret keys derived from the 120 bit user defined secret key serve as the initial condition for the chaotic sequences. Both the image and the mask for diffusion are encoded into DNA sequences using the possible eight DNA complementary rules. After that, image permutation and diffusion operations are performed in the DNA domain. DNA XOR operation is used to carry out diffusion which significantly reduces the correlation between adjacent pixels of the plain image. The results shows that the effect of DNA could improve the performance of the system in all the security aspects[8].

## CONCLUSION

In this paper, an image encryption technique is presented based on the two independent encryption procedures, which are used to protect different types of images. Compared with the single chaotic map scheme, the proposed algorithm will exhibit higher security.Due to the structure similar to the style of Feistel block cipher, the

proposed algorithm can complete the encryption of two pixel blocks at one time, which is helpful for increasing data throughput. The security analysis shows that the method can resist many forms of cryptanalysis.It can be concluded from the results that BA presents good avalanche text from the second round. However, BA has a good non-linear relation between plaintext and cipher text. Hence, for futures work, cryptanalysis of BA will be investigated on the BA. In addition, a similar analysis will be carried out on the extension of BA 128 –bit.

## REFERENCE

[1] TejalMahajan, ShraddhaMasih, "Enhancing Blowfish File Encryption Algorithm through Parallel Computing on GPU", IEEE International Conference on Computer, Communication and Control (IC4-2015).

[2] YifengZheng , Chen Wang, "A Novel ImageCascaded Encryption AlgorithmBased on Chaos withRelated Security Evaluation Scheme", IEEE, 2012, pp.768-772.

[3] Sudeshna Bora, PritamSen, ChittaranjanPradhan, "Novel Color Image Encryption Technique using Blowfish and Cross Chaos Map", IEEE, ICCSP, 2015, pp. 0879-0883.

[4] VaibhavPoonia, Dr.Narendra Singh Yadav, "Analysis of modified Blowfish Algorithm in different cases with various parameters", International Conference on Advanced Computing and Communication Systems (ICACCS -2015), Jan. 05 – 07, 2015.

[5] Garima Mehta, Malay Kishore Dutta, RadimBurget, Vaclav Uher, "Edge Based Block Wise Selective Fingerprint Image Encryption Using Chaos", IEEE, 2015, pp. 555-559.

[6] Jan Sher Khan, AtiqueurRehman, Jawad Ahmad, ZeeshanHabib, "A New Chaos-Based Secure Image Encryption Scheme Using Multiple Substitution Boxes", Conference on Information Assurance and Cyber Security (CIACS), IEEE, 2015, pp. 16-21.

[7] MinalGovindAvasare, VishakhaVivekKelkar, "Image Encryption using Chaos Theory", International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, IEEE, 2015.

[8] Saranya M R, Arun K Mohan, K Anusudha, "A Hybrid Algorithm for Enhanced Image Security Using Chaos and DNA theory", International Conference on Computer Communication and Informatics (ICCCI - 2015), Jan. 08 – 10, IEEE, 2015.