Secure Image 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 technique. The demand for fast and secure cryptographic encryption techniques has been growing over the recent year. In open network, it is important to keep sensitive information secure from becoming vulnerable to unauthorized access. Encryption is used to ensure high security for image. Blowfish Algorithm (BA) 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. Chaos has been widely used for image encryption for its different features. There are many chaos based encryption techniques. Chaotic maps gives advatnages of large key space and high level security. There are various techniques which are discovered from time to time to encrypt the images to make images more secure. In this paper; proposed system used canny method for find the maximum boundary of image. In this paper a Different Image Encryption and encryption techniques that are existing is given. It additionally focuses on the functionality of Image encryption and decryption techniques. Parameters such as NPCR (Number of Pixels Changing Rate), UACI (Unified Average Changing Intensity), and CC (Correlation Co-efficient) are used for the effectiveness of our proposed technique. The result provides a high level of security. C++ is used in the implementation of the blowfish algorithm; MATLAB programming is used in the implementation of correlation coefficient, NPCR, UACI. To evaluate security & performance, correlation coefficient, NPCR, UACI etc.

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

I. INTRODUCTION

BA was designed by schneier at the Cambridge Security Workshop in December 1993 to replace the Data Encryption Standard (DES). It has been widely analyzed and gradually accepted as a good and powerful encryption algorithm offering several advantages among which is its suitability and efficiency for implementing hardware. It is also unpatented and therefore does not require any license. The elementary operators of BA algorithm comprise table lookup, addition, and XOR with the table being made up of four S-boxes and a P-array. Based on Feistel rounds, BA is a cipher with the F-function design being a simplified version of the principles employed in DES to provide similar security, faster speed and higher efficiency in software [1]. 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. Chaos Encryption algorithm work on sequence based [2].

II. CRYPTOGRAPHY

Cryptography is an essential part for the Information Security System (ISS). It plays an important role in the security of data between sender and receiver. Cryptography provides us confidentiality, accuracy, fairness, along with data integrity. Now the cryptography is used routinely to secure data, which must be communicated and/or saved over long periods, to protect electronic fund transfers and classified communications. Modern cryptographic techniques are based on number theoretical or algebraic concepts[3].

A. TYPES OF CRYPTOGRAPHY

Mainly two types of cryptography are known: Asymmetric key cryptography and Symmetric key cryptography.

- Asymmetric Key Cryptography

In this type of cryptography, there are two keys used: public key and private key, one for encryption and one for decryption purpose. Popular examples of asymmetric key cryptography are: RSA, ElGamal, Merkle's Puzzles, Elliptic Curve Cryptography (ECC) [2]. An Asymmetric key cryptography is also known as public key cryptography. Blowfish algorithm don't need a secured beginning exchange of one or more keys between the sender and receiver. The algorithm used for encryption and decryption was designed in such a way that, it makes easy for the receiver to produce the public and private keys and to decrypt the message by private key. It is also easy for the sender to encrypt the message by utilizing public key, and it is very difficult for anyone to find out the private key based on the knowledge of the public key[3].

- Symmetric Key Cryptography

In this type of cryptography, same key is used for both encryption and decryption purpose. Symmetric algorithms can be divided into two type-stream cipher and block cipher. Stream cipher encrypt one bit of plaintext at a time as compared to block cipher which takes a number of bits (typically 64 bits), and encrypt them as one unit in whole. Symmetric ciphers are likely to be harmed by the known plaintext and chosen text attacks, as well as differential and linear. Some examples of popular symmetric algorithms are: Serpent, Twofish, AES (Rijndael), Blowfish, CAST5, RC4, RC6, DES, 3DES, and IDEA. Symmetric key algorithms are less computationally intensive as compared to asymmetric key algorithms. But in practice, asymmetric key algorithms are much slower as compared to the symmetric key algorithms. Asymmetric algorithms(also known as public-key algorithms) requires at least a 3,000-bit key to reach at the same level of security as that of a 128-bit symmetric algorithm[3].

III. 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 [4].

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-bit unsigned 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[4].

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

IV 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[5].

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[6]

For image encryption chaotic system can be represented

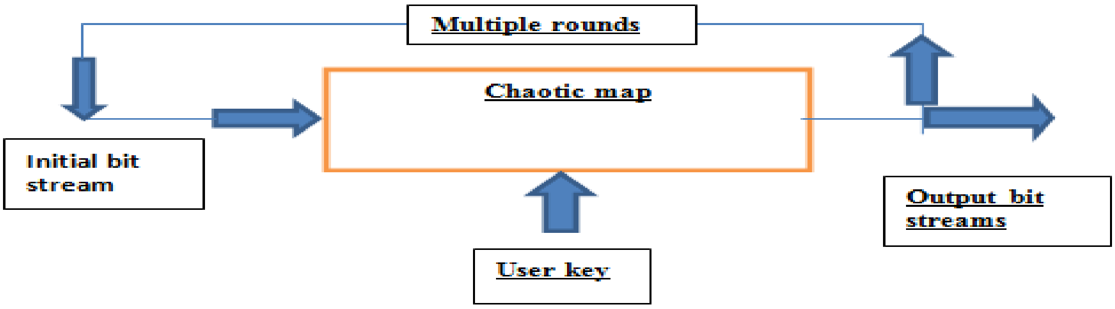

Fig 1 Chaos based encryption.[6]

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[6].

V LITERATURE SURVEY

Table -1 Comparative Study

Sr No	Paper Title	Method used	Strong Point	Weak Point
1	Analysis of modified Blowfish Algorithm in different cases with various parameters	Blowfish method	More Compact and more secure	Key sensitivity
2	Edge Based Block Wise Selective Fingerprint Image Encryption Using Chaos	Edge detection method	Data completely recover, complexities reduce	Highly key sensitive
3	A New Chaos-Based Secure Image Encryption Scheme Using Multiple Substitution Boxes	Substitution method	Defences Security attack	Highly sensitivity
4	Image Encryption using Chaos Theory	Chaos method	High level security	----------
5	Security Analysis of Blowfish algorithm	Blowfish method	Good avalanche results	------------

6	A New Chaos-based Image Cipher Using a Hash Function	Chaos method, permutation, diffusion	Good computational efficiency	------------
7	Novel Colour Image Encryption Technique using Blowfish and Cross Chaos Map	Blowfish and Chaos	High level Of security	Total time, Correlation Variation

VI PROPOSED SYSTEM

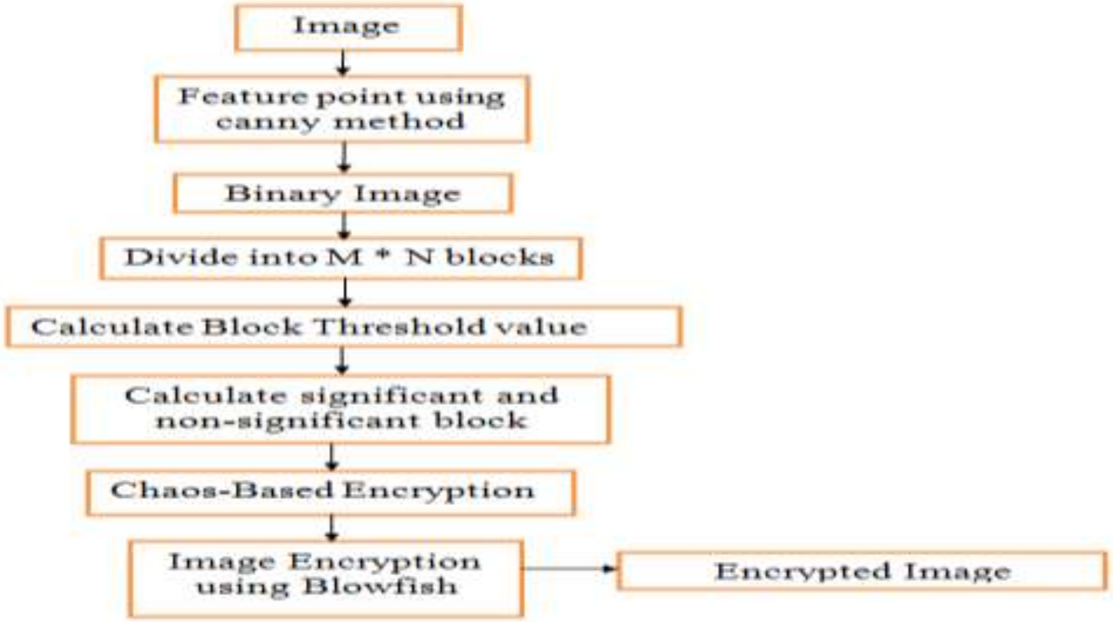
Image
Feature point using canny method
Binary Image
Divide into M * N blocks
Calculate Block Threshold value
Calculate significant and non-significant block
Chaos-Based Encryption
Image Encryption using Blowfish
Encrypted Image

Fig.4 Proposed System

In order to enhance the security and accuracy for different technique has been proposed and following are the steps. Step 1: Take the original image(Any database image or single image).Step 2: Apply pre-processing using canny method. Step 3: Output image converted into binary image.Step 4: Divide image into m*n blockStep 5: Calculate significant and non-significant block.Step 6: Apply chaos encryption technique.Step 7: Apply Blowfish encryption technique.Step 8: Retrieve encrypted image.

VII RESULT ANALYSIS

For implementation of proposed Flow work has been experimented through matrix laboratory software (MATLAB), which is running on laptop with a 2 GHz Core2duo with 2GB RAM and Windows 8 Operating System.

For experiment the 5 different images are taken for the 5 times with the same size. And the result of Number of pixels Changing rate, Unified Average Changing Intensity is given below.

By this Result we can say that NPCR_SCR IS 0.995881398518880, NPCR_PVAL is 0.001268266675230, UACL_SCR is 0.365209108240464, UACI_PVAL is 0.

Image	NPCR_TYPE	WHOLE IMAGE
Pepper	NPCR_SCR	0.995881398518880
	NPCR_PVAL	0.001268266675230

Table -2 Result of NPCR

Image	UACI_TYPE	WHOLE IMAGE
Pepper	UACI_SCR	0.365209108240464
	UACI_PVAL	0

Table -3 Result of UACI

VIII 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] Ashwak ALabaichi, Faudziah Ahmad, Ramlan Mahmod, “Security Analysis of Blowfish algorithm”, IEEE, 2013, 10.1109/ICoIA.2013.6650222, pp. 12-18

[2] Minal Govind Avasare, Vishakha Vivek Kelkar, “Image Encryption using Chaos Theory”, International conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, IEEE, 2015, 10.1109/ICCICT.2015.7045687.

[3] Vaibhav poonia, Dr. Narendra Singh Yadav, “ Analaysis of modified Blowfish Algorithm in different cases with various parameters”, International Conference on Advanced Computing and Communication Systems (ICACCS -2015), Jan. 05 – 07, 2015, 10.1109/ICACCS.2015.7324114, pp. 1-5

[4] Tejal Mahajan, Shraddha Masih, “Enhancing Blowfish File Encryption Algorithm through Parallel Computing on GPU”, IEEE International Conference on Computer, Communication and Control (IC4-2015).

[5] Yifeng Zheng , Chen Wang, “A Novel ImageCascaded Encryption AlgorithmBased on Chaos withRelated Security Evaluation Scheme”, IEEE, 2012, pp.768-772.

[6] Minal Govind Avasare, Vishakha Vivek Kelkar, “Image Encryption using Chaos Theory”, International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, IEEE, 2015.

[7] Vaibhav Poonia, 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.

[8] Vaibhav Poonia, 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.

[9] Garima Mehta, Malay Kishore Dutta, Radim Burget, Vaclav Uher, “Edge Based Block Wise Selective Fingerprint Image Encryption Using Chaos”, IEEE, 2015, pp. 555-559.

[10] Jan Sher Khan, Atique ur Rehman, Jawad Ahmad, Zeeshan Habib, “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.

[11] Minal Govind Avasare, Vishakha Vivek Kelkar, “Image Encryption using Chaos Theory”, International Conference on Communication, Information & Computing Technology (ICCICT), Jan. 16-17, IEEE, 2015.

[12] 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.