ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 1, January 2019

Image Security using Cipher Feedback Mode with Hash Function

T.Sivakumar[1], A.Selvakumar[2], M.S.Nivethini[3], R.Navami[4]

Department of Computer Science and Engineering, Dr.Mahalingam College of Engineering and Technology,

Pollachi, Coimbatore, India[1,2,3,4]

Abstract: Secured data storage and transmission has become an important issue in the digital world due to the increased use of Internet for communication purposes. Information security is becoming more important as the amount of sensitive data being exchanged on the Internet increases. The services like confidentiality and data integrity are required to protect data against unauthorized usage and modification. Visual systems help humans to understand the scenario and improve the understanding capacity. Secure sharing of images helps not only to prevent leakage of data, but also makes it difficult to retrieve the original image in case of the image falling into the wrong hands. In this paper, the cipher feedback mode with hash function has been utilized to encrypt digital images. The proposed method is experimented, tested against security attacks and the obtained results are compared with the existing methods.

Keywords: Image Encryption, Random Number, Modes of operation, Hash Function.

I. INTRODUCTION

Image encryption is vital for safely and securely transferring images by users such as the military, health care and government agencies. Most of the military organizations use readily available encryption algorithms with key lengths that vary depending on the levels of protected data's clearance. These algorithms should be made public as per kerckhoff's principle, which says that a secure cryptosystem can't rely on secrecy of the algorithm or process of encryption/decryption because a skilled attacker will shred through such obscurity and discover faults in the system. The algorithm chosen for encryption varies depending on the medium and intention. For example, unstructured and structured digital data at rest may be encrypted with AES whereas data in flight may be encrypted with skipjack. Most militaries require these algorithms to be vetted by their government's electronic intelligence or technology standards organization for security. Cryptography is the art of achieving security by encrypting messages to make them non-readable at the sender's side and decrypting the messages at the receiver's side to obtain the original information.
Random numbers can be classified as Pseudo-random number generators (PRNG), True random number generators (TRNG) and Pseudo-random Function (PRF). PRNGs are deterministic and periodic whereas PRNGs are non-periodic and periodic. Hash function is a one-way function which generators a fixed length output, irrespective of the length of the input. A PRNG is used to promote a random number as the Seed(Initialization vector). A TRNG takes as input a source that is effectively random; the source is often referred to as an entropy source. The source or combination of sources, serve as input to an algorithm that produces random binary output. It converts analog source to binary output. A PRF is used to generate a pseudo random string of bits of some fixed length. The PRF takes as input a seed plus some constant specific values such as user ID or application ID.

The rest of the paper is organized as follows. Chapter 2 presents a brief overview of the existing literature. Chapter 3 describe the methodology used to get the cipher image by the proposed method. Chapter 4 presents the experimental results and the performance analysis. Conclusion is provided in Chapter 5.

II. LITERATURE SURVEY

A. Image encryption algorithm based on hash function

A novel algorithm for image encryption based on SHA-512 is proposed. The main idea of the algorithm is to use one half of image data for encryption of the other half of the image reciprocally. Distinct characteristics of the algorithm are high security, high sensitivity and high speed that can be applied for encryption of gray-level and color images. The algorithm consists of two main sections: The rest does preprocessing operation to shuffle one half of image. The second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted. The aim of this work is to increase the image entropy. Both security and performance aspects of the proposed algorithm are analyzed and satisfactory results are achieved in various rounds .Development of computer networks leads to more convenient access to digital images through multimedia networks. Therefore much research has been accomplished on these images due to the lack of access to digital images by illegal users. Usually,

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 1, January 2019

encryption is one good way to ensure high security. Encryption is used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce, cell phones, and wireless intercom systems). The three most common cryptographic primitives used in image encryption are Block ciphers, pseudo-random number generators, and hash functions. Chaos has been used to achieve the first two primitives for more than a decade (e.g., chaos-based ciphers and chaos-based random number generators .In this paper, a novel algorithm for image encryption based on SHA-512 is presented. The proposed algorithm combines good permutation and diffusion properties in four steps per round. Due to elimination of CBC-like mode in the proposed algorithm, the image encryption can be implemented parallel [2].

B. A pseudorandom number generator with keccak hash function

It presents a pseudorandom generation algorithm, which is based on the KECCAK hash function and can pass the random test of the NIST (National Institute of Standards and Technology) Statistical Test Suite. Its security shows that can be utilized to generate pseudorandom bit sequences, which the experimental results show the KECCAK hash function has excellent pseudo randomness. The security of many cryptographic mechanisms that are used in TCPA depends upon the generation of unpredictable quantities. Example include the primes in the RSA encryption and digital signature schemes, the secret key in the DES and 3DES encryption algorithms, and the nonce used in challenge-response integrity-checking system. In all these cases, the quantities generated must be of sufficient size and be random in the sense that the probability of any particular value being selected must be sufficiently small to preclude an adversary from gaining advantage through optimizing a search strategy based on such probability. Ideally, secrets required in cryptographic algorithms and protocols should be generated with a true random bit generator. However, the generation of random bits is an inefficient procedure in most practical environments. Moreover, it may be impractical to securely store and transmit a large number of random bits if these are required in application such as the on-time pad. In such situations, substituting a random bit generator with a pseudo-random bit generator can ameliorate the problem. It about an algorithm for a pseudorandom generation number, which is based on the KECCAK hash function and can pass random test of the NIST Statistical Test Suite and ENT random test [13]

C. Image encryption based on pixel shuffling and random key stream

Secured data storage and transmission has become an important issue in the digital world due to the increased use of Internet for communication purposes. Information security is becoming more important as the amount of sensitive data being exchanged on the Internet increases. The services like confidentiality and data integrity are required to protect data against unauthorized usage and modification. In recent years, several image encryption methods are introduced by various researchers to secure multimedia information while transit via public networks. A novel image encryption method based on pixels position permutation and random key stream is suggested in this paper. The pixels position permutation is done based on Hilbert Curve (HC). The pixel shuffled image is XORed with random key stream constructed by adopting the random bit pattern procedure used in the MD5 hash function to obtain the cipher image. The volume of data that represent an image is always greater than textual messages and the traditional algorithms takes long time to encrypt digital images. Image encryption is widely used in multimedia communication, medical imaging, telemedicine and military communications where time is critical. A new image encryption method is introduced based on pixels position permutation and random key stream. The pixels position permutation is done based on the novel implementation of Hilbert Curve. The constants generation method used in the MD5 hash function is adopted to generate random key stream. The encryption method is very sensitive for the encryption key and is secure against additive noise and cropping attacks.[14]

D. Image authentication based on double-image encryption

An image authentication scheme is proposed based on double-image encryption and partial phase decryption in non-separable Fractional Fourier transform domain. Two original images are combined and transformed into the non-separable fractional Fourier domain. Only part of the phase information of the encrypted result is kept for decryption while the rest part of phase and all the amplitude information are discarded. The two recovered images are hardly recognized by visual inspection but can be authenticated by the nonlinear correlation algorithm. The optical image encryption techniques have been widely studied due to its advantage of potential fast computational processing and the parallelism achievable. The double random phase encoding (DRPE) is a classical method among various optical encryption techniques. We propose an image authentication based on double image encryption and partial phase decryption in NFRFT domain. Two original images respectively taken as the real and imaginary part of the input signal are encrypted simultaneously using NFRFT. The employment of the double-image scheme lowers the time cost due to the parallel processing of two images in one time and the partial phase mode for decryption reduces the storage and transmission costs. The proposed authentication scheme achieves respective authentication of both images by single encryption-decryption operation. In the scheme, only partial phase information of the encrypted data is preserved for decryption so that the recovered images cannot be recognized visually. However, both recovered images can be

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 1, January 2019

authenticated using the nonlinear correlation algorithm. The security level of the cryptosystem increases because the recovered images cannot be recognized by direct visual inspection [1].

E. Fast Image Encryption based on Random Image Key

There is no doubt that information technology plays a significant role to support the computer applications to many users and establishments in the world like information security, information hiding and information retrieval. As a matter of fact, all users, who use multimedia such as image, audio, video and text, may need to protect information from attacks during sending or receiving them through channel. There are two challenges for multimedia encryption; the first one is the size of data and the second is the cost of encryptions [1]. Image Cryptosystem can be classified into two main sections; one for encryption and the other for decryption. The block cipher and stream cipher are two types of cryptosystem, so private key and public key are two strategies to be used in an encryption. In this paper a new algorithm is proposed to encrypt color image using symmetric key which is generated from the same image or any image can be selected. Some tests are applied here to determine performance algorithm. These are histogram, mean square error, peak signal to noise ratio, entropy, correlation coefficients, number of changing pixel rate and unified averaged changed intensity [2]. The proposed algorithm was satisfied with good results where speed of running was good for encryption and decryption algorithm. [15]

III. THE PROPOSED IMAGE ENCRYPTION METHOD

The block diagram shows the basic algorithm overview of the image encryption. A random key stream is generated using the cipher feedback block(CFB) and the number of bits generated by each image block is matched with the selection box of the CFB. An XOR operation is performed between scrambled image and random key stream to obtain the cipher image. The final cipher image is stored in a file. The cipher generated is used for the next number of bits and this repeats till all the blocks have been encrypted

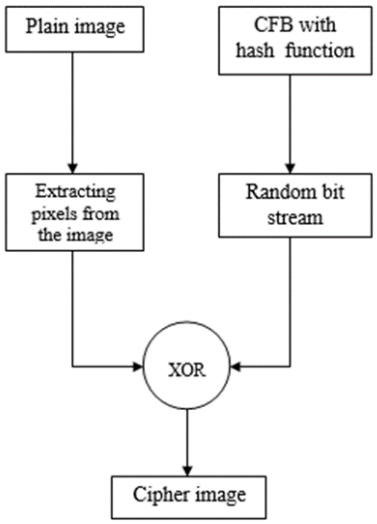


Figure 1: Sequence of steps involved in the proposed image encryption process

A. Cipher feedback block with hash function

The existing method of CFB uses an encryption algorithm which is typically DES or AES to generate an encrypted mode of the initialization vector which is then used for the rest of the algorithm. The proposed method uses hash function instead of contemporary encryption methods to encrypt the IV (initialization vector) or the key. The key is set by the user and has to be known to both parties. The hash of IV is the sent to the selection box which selects the bits to be XOR with the plaintext to generate the cipher text.

B. Encryption Process

The input image is divided into blocks of 32 bytes to match the size of the resultant hash from MD5.A user input key is fed to an MD5 function which results in the hash of the key. An XOR operation is performed between a block of the original image and the hash value. This is repeated multiple times till the entire image is encrypted. The XORed value of the first block is hashed again and used to XOR the next block, which forms the feedback functionality.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 1, January 2019

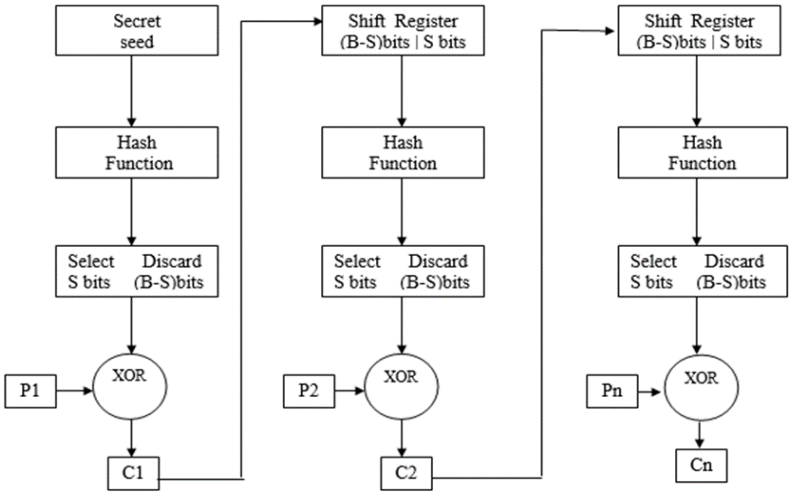


Figure 2: Block Diagram of Encryption.

C. Decryption Process

The same method is followed for the decryption sequence. The key is received from the user, which is hashed. This hash is again used to XOR the first 32 bytes of the image. The result of this is hashed and again used to XOR with the next 32 bytes. This is repeated till the whole image is decrypted

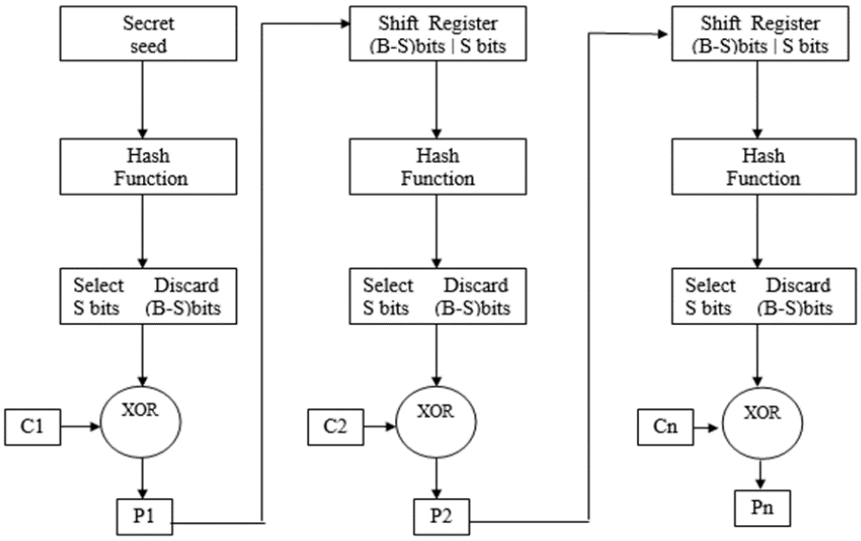


Figure 3: Block Diagram of Decryption.

IV. EXPERIMENTAL RESULTS & ANALYSIS

The proposed method is implemented using JDK 1.8 with JCE (java cryptographic extension) with Intel core i5 processor, 2.0 GHZ , 8 GB ram,500 GB HDD and windows 10(64 bit) operating system. The proposed method is experimented with images of sizes: 256*256, 512*512 pixels.

The java program uses java imageio and crypto packages from JCE to encrypt the content of the image. Java is used to facilitate the extraction of pixels from the image.

A. Experimental Results

This approach is tested with different gray scale images of size 256x256 pixels. Sample input images are shown in Figure 4 & Figure 5

.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

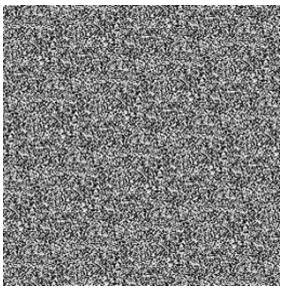
International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 1, January 2019

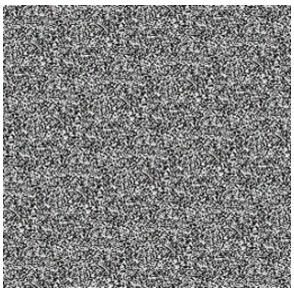
Figure 4: Input Image1

Figure 5: Input Image2

The sample random number generated using the proposed method is shown in Figure 6(a) and the obtained encrypted image is shown in Figure 6(b).



(a) Sample random numbers



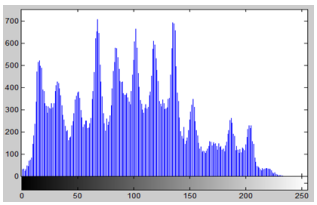
(b) Encrypted image

Figure 6: Result of the Proposed Image Encryption Method

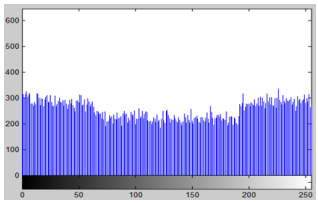
B. Result Analysis

1) Histogram

The histogram analysis clarifies that, how the pixel values of image are distributed. The histogram of original image contains great rises followed by sharp declines and the histogram of encrypted image has uniform distribution which is different from the original image. Figure 6 shows the histogram of the original and the corresponding encrypted images.



(a) Original Lena image



(b) Encrypted Lena image

Figure 7: Histogram of Lena image

2) Correlation

Correlation computes the degree of similarity between two variables. This parameter is useful for measuring the effectiveness of the cryptosystem. An arbitrarily chosen pixel in an image is generally strongly correlated with adjacent pixels, and it's in horizontal, vertical or diagonal directions. A secure image encryption algorithm must produce an encrypted image having low correlation between adjacent pixels. The correlation coefficient is calculated by using the Equations (1) to (4).

$$\gamma_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (1)$$

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))(yi - E(y)) \quad (2)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(xi - E(x))^2 \quad (3)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}x_i \quad (4)$$

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 1, January 2019

Where, Cov(x, y) is the covariance of x and y; x, y are values of adjacent pixels in image, N is the number of pixel pairs (xi, yi), and E(x) and E(y), are the mean values of xi and yi respectively.
The result attained by proposed method and few existing methods are given in Table 1.

Table 1.Comparison of Adjacent Pixel Correlation

Encryption Method	Encrypted Image		
	Horizontal	Vertical	Diagonal
Proposed	0.0246	0.1142	0.1241
Narendra k Pareek [3]	0.0083	-0.0162	0.0078
G.A.Sathishkumar [7]	0.0083	0.0162	0.0078
T.Sivakumar [9]	0.1366	0.1498	0.0225
T.Sivakumar [14]	0.0045	0.0073	0.0241

3) Information entropy

The entropy of gray-scale images is theoretically equal to 8 Sh, if each level of gray is assumed to be equiprobable. If the entropy values of the encrypted images are close to the ideal value of 8 Sh, then the encryption algorithm is highly robust against entropy attacks. The entropy of the information is computed by using the Equation (5).

$$H(m) = \sum_{i=0}^{m-1} p(mi) log\left(1/p(mi)\right) \qquad (5)$$

Where, m is the total number of symbols in mi∈m; p (mi) represents the probability of occurrence of the symbol mi and log denotes the base 2 logarithm. The obtained entropy value of the proposed method and few existing methods are given in Table 2. It is observed that the result obtained by the proposed method is acceptable and comparable with the existing methods.

Table 2. Comparison of Entropy Value

Encryption Method	Entropy Value (Sh)
Proposed	7.8844
Narendra k Pareek [3]	7.9996
G.A.Sathishkumar [7]	7.8101
T.Sivakumar [14]	7.9924

CONCLUSION

In this paper, the cipher feedback mode with hash function had been utilized to encrypt digital image. The idea is to use a one-way function instead of the existing encryption algorithms to speed up the process of image encryption. The hash function with cipher feedback mode is used to generate the random numbers. Further, the random numbers are XORed with the original image to get the cipher image. The proposed method in experimented, tested against security attacks and verified with the obtained result.

REFERENCES

[1]. Linyuana, qiwenrana, Tieyu Zhao, “Image authentication based on double-image encryption and partial phase decryption in non-separable fractional Fourier domain”, optics and Laser Technology, 88, 111-120, 2017.
[2]. Seyed mohammad seyedzade, rezaebrahimiatani, sattarmirzakuchaki, “A novel image encryption algorithm based on hash function”, Machine vision and image processing, pp. 1-6, Oct 2010,
[3]. Narendra k pareek, “Design and analysis of a novel digital image encryption scheme”, international journal of network security & its applications, 2012.
[4]. Abbas cheddar, joancondell, Kevin Curran, Ppaulmckevitt, “A hash-based image encryption algorithm”, optics Ccommunications, p. 879-893, Vol. 283(6), 2010.
[5]. Robin fay,”Introducing the counter mode of operation to compressed sensing based encryption”, Information proceeding letters, p. 279-283, 116(4), 2016.
[6]. Kinga matron, A lin Suciu, Christian săcărea, Octavian ret, “Generation and testing of random numbers for cryptographic applications”, Romanian academy, series A, volume 13, number 4, pp. 368–377, 2012.
[7]. G.A.Sathishkumar and K.Bhoopathybagan,”A Novel Image Encryption Algorithm Using Pixel Shuffling and BASE 64 Encoding Based Chaotic Block Cipher”, ISSN: 1109-2750, Issue 6, Volume 10, June 2011.
[8]. Abdulrahman Dira Khalaf, ”Fast Image Encryption based on Random Image Key”, International Journal of Computer Applications, 975:8887, 2016.
[9]. T.Sivakumar and R.Venkatesan, “A Novel Image Encryption Approach using Matrix Reordering”, WSEAS Transactions of Computers, Vol. 12, Iss. 11, Nov 2013.

[10]. Andrew Rukhin,Juan Soto, James Nechvatal, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications National Institute of Standards and Technology", Special Publication 800-22 revision 1a Natl, vol:131, April 2010.
[11]. Sheng Yuana, Yangrui Yanga, Xuemei Liua, Xin Zhoub, Zhenzhuo Weia, "Optical image transformation and encryption by phase-retrieval-based double random-phase encoding and compressive ghost imaging", Optics and Laers in Engineering, pp. 105-110, 100, 2018.
[12]. Zhengjun Liua, Hang Chenb, Walter Blondel, Zhenmin Shene , Shutian Liuf, "Image security based on iterative random phase encoding in expanded fractional Fourier transform domains", Optics and Lasers in Engineering, pp. 1-5, 105, 2018.
[13]. A. Gholipour S. Mirzakuchaki ,"A Pseudorandom Number Generator with KECCAK Hash Function", International Journal of Computer and Electrical Engineering, Vol. 3, No. 6, December 2011.
[14]. T. Siva Kumar and R Venkatesan, "Image Encryption Based on Pixel Shuffling and Random Key Stream", International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 03 – Issue 06, November 2014.
[15]. S.S. Maniccam and N. G. Bourbakis, "Image and video encryption using SCAN patterns", Pattern Recognition, Vol. 37, No. 4, pp725-737, 2004.
[16]. Xin Ma, Chong Fu, Wei-min Lei and Shuo Li, "A novel chaos-based image encryption scheme with an improved permutation process", International Journal of Advancements in Computing Technology, Vol. 3, No. 5, pp 223-233, 2011.
[17]. Yue Wu, Joseph P. Noonan and Sos Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Journal of Selected Areas in Telecommunications, pp.31-38, 2011.
[18]. N.K. Pareek, Vinod Patidar, and K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing , Vol. 24, pp. 926-934, 2006.
[19]. Pratibha S. Ghode, "A Keyless approach to Lossless Image Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 5, pp 1459-1467, 2014.