ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Survey on New Image Encryption Algorithm Based on Diffie-Hellman and Singular Value Decomposition

Tambe Chaitali A[1]., Gadilkar Rupali S[1]., Pawar Vimal T[1]

B. E. Student, Dept. of Information Technology, PREC, Loni, Ahmednagar, Maharashtra, India[1]

ABSTRACT: With the fast progression of using images in many applications, it is important to protect the confidential image data from unauthorized access. This paper weproposed a new way to encryption image based on few steps: the first one aims to scrambling the image values by using Fibonacci transform, while the another step focus on generating public & private key based on Diffie-Hellman Key Exchange, these keys used to encrypt the diagonal matrix which created by Singular-Value-Decomposition (SVD) in third step. Decryption is the inverse process of encryption. The results were promised and the decrypted image retrieved without loss any of its information. Encryption and decryption time was very trivial. The contribution of this paper is to encrypt image by using singular value decomposition with Diffie-Hellman Key Exchange. Paper novelty based on scrambling values based on Fibonacci transform and encryption image by using SVD.

KEYWORDS: Decryption, Encryption, DH, Fibonacci, SVD.

I. INTRODUCTION

With the increasing growth of the multimedia applications, security is an important issue in transmission of images. Encryption is one the way to ensure security. Image encryption techniques convert original image to another image which is hard to understand. Also reliable security in storage and transmission of digital images is needed in many applications, such as online personal photograph album, medical systems, confidential video conferences, military communications etc. In order to fulfill such a task, many image encryption methods have been proposed. Encryption is the part of encoding messages & information in such a way that only authorized parties can able t o read it using the decryption key. An authorized person can easily decrypt the message with the key provided. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information.

There are too many methods suggested each day to keep the data secure, but the problem is hackers and unauthorized persons continues trying to crack those methods. Nowdays, data security is a important in data storage and transmission. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Image encryption plays a significant role in the field of information hiding. The important different between image encryption and text encryption is the image size which is almost always much greater than the text size. For that the use of traditional cryptosystems need much time to encrypt the image. The other different is related to decryption, the decrypted image allowed to some changing from the origin image while this case not allowed in text decryption.With the rapid increase in the development of advanced network technology, multimedia information is transmitted openly over the Internet conveniently and encryption of such data is very crucial. Various confidential data such as, image data from unmanned Ariel vehicles, military maps and video from remote devices need to be secured. There have been a lot works done in pixel displacements at the software level which have to do with internet multimedia applications and some implementations at the hardware level.

DOI: 10.15680/IJIRCCE.2017. 0501102

II. RELATED WORK

1. Image Encryption via Prediction Error Clustering and Random Permutation

The proposed work is to present an image encryption-then-compression (ETC) system, where both lossless and lossy compression is considered. We implement image encryption themes operated in the prediction error domain to provide a reasonably high level of security. Also an efficient compression of the encrypted images is performed and compared with unencrypted image compression efficiencies [1].

2. Lossless Compression of Encrypted Image via Adaptive AC

Most commonly, image encryption has to be conducted prior to image compression. This has led to the problem of how to design a pair of image encryption and compression algorithms such that compressing the encrypted images can still be efficiently performed. is a highly efficient image encryption-then-compression (ETC) system. The proposed image encryption scheme operated in the prediction error domain can able to provide a high level of security. An arithmetic coding-based approach can be used to efficiently compress the encrypted images. Most of the existing ETC solutions induce significant penalty on the compression efficiency[2].

3. Sequential Decryption and Decompression

In recent days transmitting digital media having large size data through the internet became simple task but providing security and security became big issue these days. Using pseudorandom permutation, image encryption is obtained. Confidentiality and access control is done by encryption. We proposed image encryption scheme operated in the pre diction error domain is able to provide a reasonably high level of security. More notably, the proposed compression approach applied to encrypted images is only slightly worse, unencrypted images as inputs [3].

4. An Image Encryption Method: SD-Advanced ImageEncryption Standard: -

The security of digital information in modern times is one of the most important parts to keep in mind. For this reason, in this paper, the author has proposed a new standard method of image encryption [4]. The proposed system following 4 different stages: 1) First, the number is to generated from a password and each pixel of the image is to converted its equivalent eight binary number, and in that eight bit number, the number of bits, which are equal to the length of the number generated from the password, are rotated and reversed; 2) In second stage, extended hill cipher technique is applied by using involuntary matrix, which is generated by same password used in second stage of encryption to make it more secure; 3) In third stage, generalized modified Vernam Cipher with feedback mechanism is used on the file to create the next level of encryption.

III. PROPOSED ALGORITHM

A. *DIFFIE -HELLMAN KEY EXCHANGE (DH):*

The DH scheme was first proposed by Whitfield Diffie and Martin Hellman in 1976, it is one of the first key exchange algorithms that is still used to this day Suppose there are two parties A and B, with C trying to snag the key through the insecure communications channel.

- The first step is to suggest a large prime number n and a nonzero integer gthat approved by both A and B. Both n and g has no need to be kept secret, so C might know them.
- In the second step A pick a secret integer (a) that is kept secret, even to B. Also B picks another integer (b) that is also kept secret to A.

A computes X=gamod n
B computes Y=gbmod n
A send X to B and B send Y to A

A computes x=Yamod n
B computes y=Xbmod n
Now x and y should be the same,
because x=Yamod n =(gb)amod n = gbamod n = gabmod n = (ga)bmod n =Xbmod n= y This shared values is now regard as encrypted key. C can only know the shared values but will be useless since C doesn't know the secret numbers (a) and (b).

B. *SINGULAR VALUE DECOMPOSITION (SVD):*

For any given matrix $A\in Rm\times n$ there exist the singular value decomposition matrices such that Orthogonal matrix of size $m\times m$, V orthogonal matrix of size $n\times n$ and S diagonal matrix of size $m\times n$ where all the entries $sij$are 0 when $i\neq j$.

$\boldsymbol{Amn=UmmSmnVnnT}$

Where $UTU=I,VTV=I$ and $s11\geqslant s22\geqslant\cdots spp\geqslant 0$,

Where p = min {m, n}. The columns of U are orthonormal eigenvectors of AAT, the columns of V are orthonormal eigenvectors of ATA, And S is a diagonal matrix containing the square root of Eigen value from U or V in decreasing order. If matrix$M$ is 5×3 this would look like $M=U\times S\times VT$.

C. *ENCRYPTION METHOD*

Encryption will follow the following steps:

(1) The input image will be read as a matrix X. For best result it is better to process the image as square image, for that the image or the matrix will be transform to square matrix (image) if it is not square.

(2) Change the elements of the matrix X randomly by using Fibonacci Transform to get matrix B.

(3) Convert the matrix B to three matrices by transform it with SVD transformation as following

$U,S,V = SVD\ (B)$…………..(4)

(4) Split the Diagonal matrix S into two Diagonal matrices A and P where the matrix A contain only integer part of S values, and matrix P contain only fractional part of S values, where:

(5) By suggestion two keys (large key and small key) to exchange with the receiver, we can create private key to use in the encryption process.

(6) Encrypt the matrix A with HD method based on private key created in the step 5. The result of this step is the matrix$F$.

(7) Now, the matrix F will be replaced instead of matrix A in relation (5) to build new matrix G as in the following relation:

$G=F+P$

(8) The final step in encryption process is to build the encrypted matrix X' by using the same matrices resulted from SVD (U and V) and the diagonal matrix (relation 6), which encrypted in the step7 as follow:

$H=U*G*VT$………… (7)

(9) Final step is option.

To increase the encryption complexity we add new key (small value).The new key subtracted from the matrix H to get new matrix D.Matrix D will be split to two equal matrices (Z and W), where Z is: $Z=mod(D,256)$

And W is: $W=Fix(D/256$

Then the final encrypted matrix is the matrix resulted from merging the two matrices (Z and W) according to the previous agreement between the sender and receiver. The result can view as image and send to the receiver.

IV. SYSTEM ARCHITECTURE

Proposed system architecture consists of image encryption at the user side and data compression at the network side. Same process of data decompression and data decryption by the user. This will achieve the security and also low data uses for the sending that data over the internet. There are many researches in this context, we select some of them which are most related: Nidhal El Abbadi, proposed new encryption algorithm based on scrambling the image data according to suggested keys (two sequence scrambling process with two different keys) which ultimately produce two different matrices. The diagonal matrix from the SVD of the resulted two matrices will be interchanged

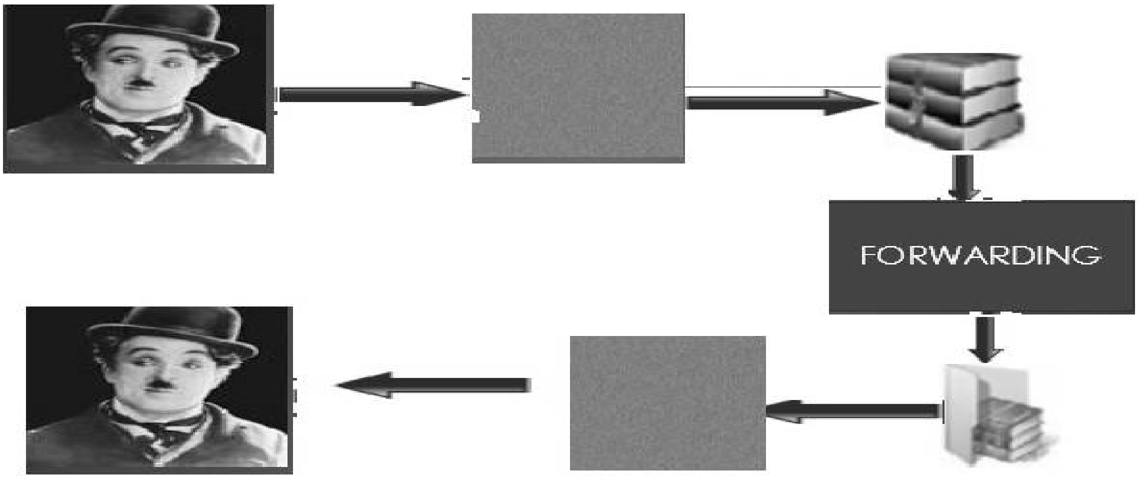

Figure 1. System architecture

Another scrambling and diagonal matrices interchange will apply to increase the complexity. Chao-Wen Chan, apply Diffie and Hellman (DH) key agreement method and total auto-morphism (TA) such that visual cryptography can be reused. Both secret and symmetry key are represented in binary image. Rinki Pakshwar described a method for new digital image scrambling method based on Fibonacci numbers. The standardization and periodicity of the scrambling transformation are discussed. The scrambling transformation has the following advantages: Encoding and decoding is very simple and they can be applied in real time situations. The scrambling effect is very sensible, the data of the image is re- distributedrandomly across the whole image.

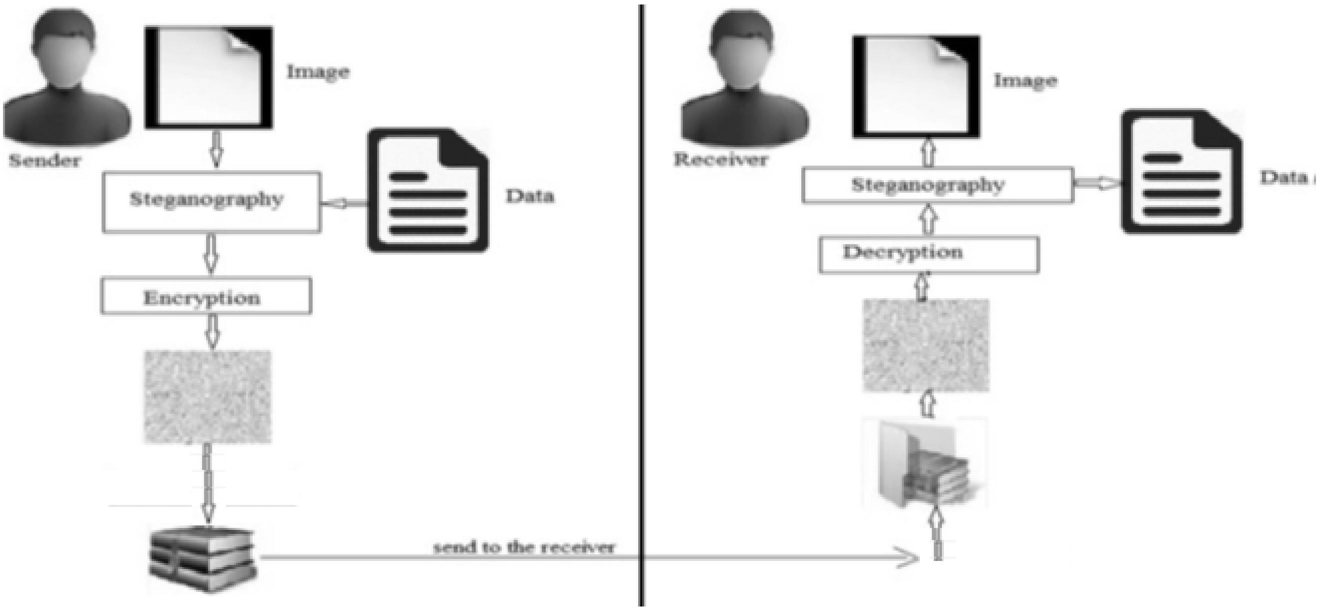

Figure 2: Compression of data

V. CONCLUSION AND FUTURE WORK

In this paper, a new improved approach for image encryption using a combination of DH and SVD techniques is proposed. The proposed method uses concept of uniform scrambling based on Fibonacci transform. Public and private keys generated based on Diffie-Hellman Key Exchange, these keys used to encrypt the diagonal matrix which created by Singular Value Decomposition (SVD).

REFERENCES

[1] Chao-Wen Chan and Yi-Da Wu, 2008, “A Visual Information Encryption Scheme Based on Visual Cryptography and D-H Key Agreement Scheme”, International Journal of Computer Science and Network Security, vol.8,no.4. 2008.
[2] HiralRathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma,“Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)”,International Journal of Computer Technology and Electronics Engineering,vol. 1, issue 3. 2011.
[3] Komal D Patel, SonalBelani, “Image Encryption Using Different Techniques: A Review”, International Journal of Emerging Technology and Advanced Engineering, vol. 1, issue 1. 2001.
[4] El Abbadi Nidhal, Adil Mohamad and Mohammed Abdul-Hameed, “Image Encryption Based on Singular Value Decomposition”, Journal of Computer Science 10 (7), pp. 1222-1230, 2014.
[5] Ozturk, I. and Sogukpınar I., “Analysis and comparison of image encryption algorithms”. International Journal of Computer, Electrical, Automation, Control and Information Engineering, Vol. 1, No. 3, 2007.
[6] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, “A Survey On Different Image Encryption and Decryption Techniques”, International Journal of Computer Science and Information Technologies, Vol. 4,issue 1, pp. 113 – 116, 2013.
[7] Somdip Dey, “An Image Encryption Method: SD-Advanced Image Encryption Standard: SD-AIES”, International Journal of Cyber- Security and Digital Forensics, vol. 1, issue 2,pp. 82-88, 2012.
[8] B. Kolman and D. Hill , 2008, "Elementary Linear Algebra With Applications", Pearson Education, Inc., Ninth Edition.