Helical and Session Based Transposition with Key Wrapping for image Encryption and Decryption

Tanu Shree Dhiran[1#]

[1]tanushree273@gmail.com

[1#]Assistant Professor, Department of Computer Engineering, Poornima University, Jaipur, India

Pratish Rawat[2]

[2]pratishrawat@gmail.com

[2]Assistant Professor, Department of Mechanical Engineering, Poornima University, Jaipur, India

***Abstract*— Network security is a primary issue while exchanging the images over the system. Exceptional and dependable efforts to establish safety are required away and various usage of transmission of computerized images, for example, paytv, medical imaging frameworks, military image communications and confidential video conferences and so forth. With a specific end goal to defeat such security issues a few image encryption strategies have been proposed, however every one of them don't give security in all cases. Consequently need to grow increasingly secure picture encryption systems are dependably in need.**

In this paper a comprehensive approach is proposed where the image file is considered as a stream of bits. Images are assembling as grids of different variable sizes. Helical and Columnar transposition is used to transforms each grid into encrypted grid. By using public key algorithm like RSA, generated key is also wrapped up. We required a private key for decryption the anti-Helical transposition. With the help of decrypting the wrapped key with receiver's private key we get session key. This method is provides the supports a variable size grid and secure variable length key.

Keywords— **Cryptography, Helical transposition, Session Key, Key Wrapping.**

I. INTRODUCTION

Inferable from the advances in network technologies, data security is an undeniably essential issue. Well known uses of mixed media innovation and expanding transmission capacity of system progressively lead us to pick up data straightforwardly and obviously through pictures. Subsequently, image security [1, 2] has transformed into a basic and significant issue. Encryption method intends to change over image to another image that is difficult to distinguish; to keep the image private between clients.

In other word, it is essential to have a decryption key without it nobody could get to know the content encrypted with that image. Till now numerous encryption and decryption algorithms [6, 7, 8, 9, and 10] are proposed but each has their own limitations. So it always required an important aspect is more reliable and secure algorithms.

In this paper an expanded system is proposed for the binary image document. The previous system [1] is executed for the .txt records. In this paper the image document is considered as a stream of bits which are formed as grids of variable sizes. The strategy changes each grid into every network by applying bit versions [3, 4, and 5]. For better security RSA method is utilized. This algorithm wraps the key with the cipher image. One of a kind image can be recovered with the help of decryption algorithm.

II. Methodology

1. Source file contains binary data which is used to construct a square grid of required size. We are taking a 32 * 32 grid, padding with 0 if essential.

2. This matrix is converted by helical manner start with bottom corner and up to middle. Helical transpositions are of 8 types. A secret key is generated with each session as combination of 0's and 1's depends on the grid size, say 32 sized is of 160-bit ,64 sized of 384- bit etc. Accordingly columnar transposition is done on the grid.

3. After the procedure of transposition new grid is generated.

4. These steps are repeated until the total file is formed into grids and encrypted. Padding with 0's is done in grid formation deficiency.

5. Key generated for each file is encrypted with the public key of sender using RSA Algorithm. This technique of hiding the key is known as key wrapping.

6. The encrypted key is then divided into various blocks and added to file. Thus, the new encrypted file with wrapped key is produced.

7. At the receiver side cipher image is converted into original image using decryption algorithm.

8. Receiver will decrypt the cipher data using his/her private key. As the session key is wrapped up with the cipher data, this will also be recovered.

9. The receiver will perform anti Helical and reverse columnar transposition to get the original image with the help of the session key.

III. Proposed Work

The working structure of the proposed techniques is as follows

This technique takes image file and forms the raw data into different grids of sizes say 32, 64, 128… by reading the binary data as bytes. The 2- dimensional array of equal size is a grid. The size of the grid is fixed for a file for each session. If the grid is not filled with data from the file, added the Padded bit 0's. Thus, the Helical and Columnar transposition encrypts the formed grid. This procedure is used to form all grids. Now a sequence of bits is generated that varies with grid size as a grouping of 0's and 1's. The different key generated at each session for a given file is different and size of grid is depending on key size. With the help of RSA Algorithm we can encrypt the session key. At this step generated key is secured from intruders. The size of grid is depending on the size of key if it is small than key is also small. Fig. 1 shows a pictorial representation of proposed work.

A. Encryption Technique

In this procedure image encryption is divided into 3 Phases.

1) Helical Transposition

2) Columnar Transposition

3) Generation of Session Key

1) Helical Transposition: This type of transposition is applied to the binary stream of the image file. In this work an algorithm is planned for binary image. 32 X 32 is the grid size. Now the Helical transposition will be implemented as follows:

Transposition is done from right bottom corner at first and at last at the position of middle. This particular image file of 32 X 32 is read in bottom to top approach but stored in a helical manner [1]. The Reading can be shown by fig 2. The binary data read as shown in fig 2 is transposed in helical manner and is stored in a new grid of equal size. So from the bottom right corner we start to write some of data streams from bottom right corner and ends in the center of the newly generated grid. A graphical representation of how the data is stored in the new grid is shown in fig 3.

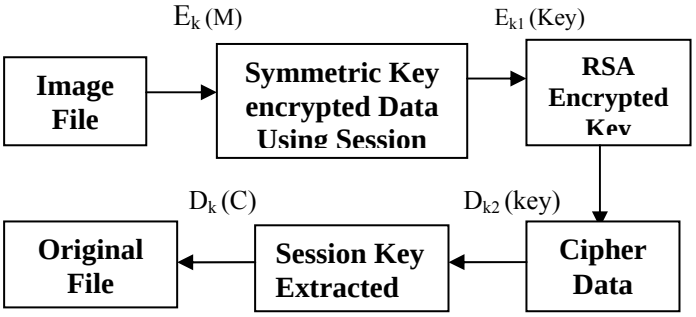

Figure 1: Graphical representation of proposed work

2) Columnar Transposition: In a columnar transposition, the rows of fix length containing message, and then read out from column by column repetitively, and then jumbled order is chosen for any of one column. At this step a session key will be generated and key is used to perform columnar transposition.

3) Generation of Session Key: Suppose if we are working on a grid of size 32 X 32, then each session key will be of 5 bits. In that way the total size of the session key for grid size 32 will be 32X5=160 bits. Similarly we can say that if the size of grid is equal to 64, then 6 bits will be required for each index. In that way the total size of the session key for the grid size 64 will be 64 X 6=384 bits. So the columnar transposition is performed according to the session key generated. This process is applied for all the grids. The resultant grid is the encrypted file.

B. Wrapping of Key

The session key is encrypted based on the public key cryptography. In this work we are proposing encryption of the session key. Each session key is considered and is encrypted by using the RSA algorithm. Each encrypted key requires 32 bits to be stored. So a grid of size 32 needs a space of 1024 bits to store the encrypted key.

RSA Algorithm: The scheme developed by Rivest, Shamir and Adleman makes use of an expression with exponentials. Blocks are encrypted form of plain text, with each block having binary values less than some number n. Encryption and decryption are of the following form, for some plain text block M and cipher text block C:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver know the value of n. The sender knows the value of e, and only the receiver knows the value of d.

So we have public key KU= {e, n} and a private key KR= {d, n}.

1. Assume any two prime numbers P, Q
2. Calculate N = P * Q
3. Calculate Z= Φ (N) = Φ (P * Q)
= Φ (P) * Φ (Q) (According to modular arithmetic) = (P-1) * (Q-1)
4. Assume a value ‘e’ i.e. relatively prime to Z and e < Z and GCD (e, Z) = 1
5. Calculate d, such that e * d ≅ 1 (mod Z) ≅ 1(mod Φ (N))

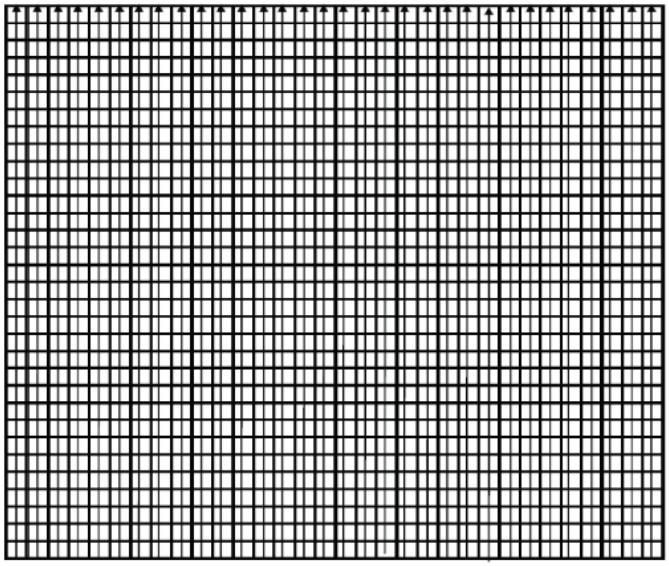

Fig. 2 Reading of binary data from the grid

6. Cipher (C) = (m ^ e) mod N Plaintext (m) =

(C ^d) mod N
Thus our key generated is both complex and secure.

C. *Decryption Technique*

Reverse process can be applied to achieve the decrypted text. The individual bytes from the file are combined and the combined result is decrypted using the private key at receiver's side. Hence the session key is obtained. The reverse process is done i.e. columnar retransposition and anti-Helical transposition to get the original image.

IV. CONCLUSION

In this paper we have planned an enhanced algorithm for the encryption and decryption of binary images. Here the cascaded Helical and Columnar Transposition which we have applied on the grid make it more secure against various cryptographic attacks. Due to padding (with 0) the decrypted image may vary from the original image but this will not produce any serious changes in the image. The session key generated is encrypted using the RSA algorithm. Using this algorithm the security of key enhanced.

V. FUTURE SCOPE

This method is used to implement for binary image files. In future this procedure can be applied on colored images, audio and video files etc. With respect of asymmetric key in place of RSA another feature enhancement of this method will be implemented. So we can have asymmetric key rather than public key or symmetric key.

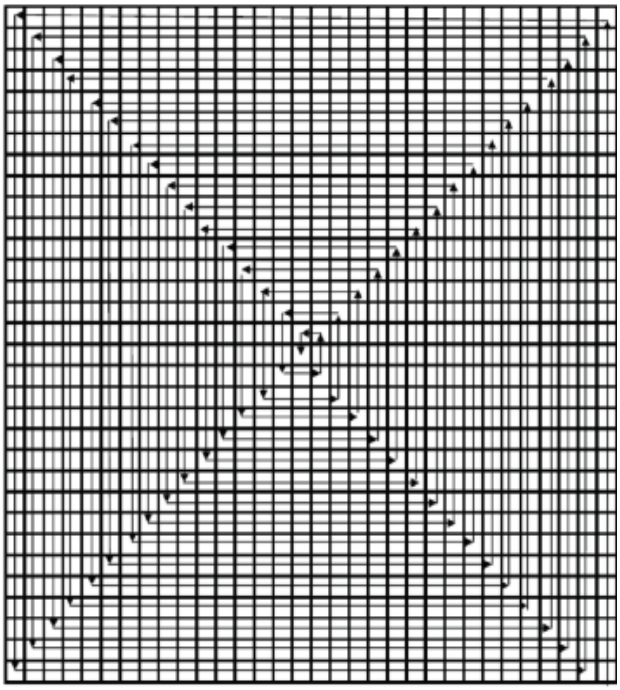

Fig. 3 storing the data in Helical Manner

REFERENCES

[1] J. Breckling, Ed., *the Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[2] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[3] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[4] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[5] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[6] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[7] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[8] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[9] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[10] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[11] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.