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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

Tutorial Review on Image Hiding

Ravindra B. Prajapati

Assistant Professor, Dept of Mechatronics-Electrical and Electronics, ITM Vocational University, Vadodara, India

Abstract: In the world of digitalization, security of image documents is bigger challenge particularly in era of image processing and analysing. Fast security system is most required in many applications like uploading private profile image, medical imaging system, and military database. And one of the ways to get higher security is encryption. Encryption is technique which convert original image to another image that is hard to understand and to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. In this paper, we survey many different encryption techniques through which we can easily hide or transfer our important document.

Keywords: Digital image Processing, image encryption, encryption key, image decryption

I. INTRODUCTION

Now a day security and integrity of data is the main concern. In the present trends all the data is transferred over computer networks due to various kind of attacks for that purpose we must encrypt the data before it is transmitted or store. Basically Image Encryption means that, convert the image into unreadable format. Encryption is used in many application like hospitals, geographical areas, military and financial institutions. If the encryption fails confidential images like enemy position, patients, and geographical areas fall into wrong hands, so it might be created disaster.

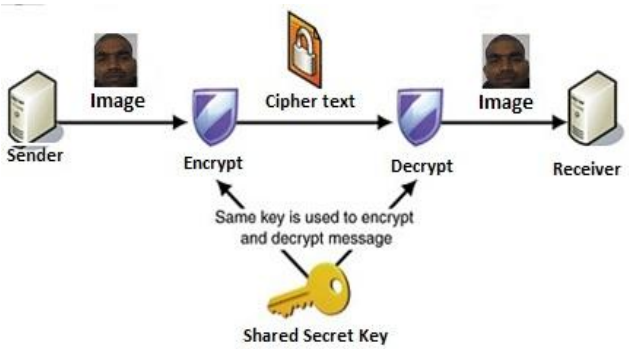

Fig. 1 Basic Block Diagram of Image Encryption

Image Encryption [1] uses a finite set of instruction called an algorithm to convert original message, known as plaintext, into cipher text, its encrypted form. Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data. With the help of key and the algorithm we can encrypt or Decrypt the plaintext into cipher text and then cipher text back into plaintext. Based on key encryption divided in two categories [2]

1. **Private Key cryptography:** Basically in this type of cryptography secret keys are shared via secure channel means only receiver have access to open the massage which is encrypted by sender.
2. **Public Key cryptography:** unlike the private key cryptography secret are not shared via secure channel instead, each party has a pair of keys called private and public keys. The public key for encryption is announced openly while the private key for decryption kept highly secret.

The Hill cipher (HC) algorithm is a famous and well known symmetric key algorithms in the era of cryptography. It is first introduced by the mathematician Lester Hill in 1929 in the journal of mathematics. It is a poly-alphabetic cipher based on linear algebra. Hill cipher requires a matrix based polygraphic system [3] [4].

In this paper, review of basic concept and different well known technics of image encryption are done by various scientist to improve the performance.

II. LITERATURE SURVEY

In 2001, Chin-Chen Chang et al [5] proposes method based on vector quantization for image encryption. This technic contain three phases.

1. In encryption phase: vector quantization is applied for compressing the original image into a set of indices.
2. In transmission phase: set of indices and encrypted data sent with a secret key to receiver by a public transmission channel.
3. In decryption phase: receiver can decrypt the encrypted data using the secret key.

In 2003, Chang-Mok Shin et al [6] suggested a multilevel image encryption by using binary phase XOR operations and image dividing technique. Algorithm steps are as follow.

1. Divide a multilevel image to binary images having equal grey intensity.
2. Binary image is transferred to binary phase encoding and these images are encrypted with binary phase images by using binary phase XOR.

In 2004, Shujun Li et al. [7] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, they conclude that secret permutations combined with other encryption techniques to create secured images.

In 2006, Mitra A et al. [8] have presented random combinational image encryption approach. The main idea behind their work is that an image can be viewed as an arrangement of bits, pixels and blocks. Perceivable data can be overcome by decreasing the correlation among the bits, pixels and blocks using permutation methods. They

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

observed that the permutation of bits is effective in significantly overcoming the correlation thereby decreasing the perceptual data, whereas the permutation of pixels and blocks are good at producing higher security then bit permutation.

In 2009, Bibhudendra Acharya et al proposed advanced Hill (AdvHill) cipher algorithm [9]. Which uses an Involutory key matrix for encryption. They observed that original Hill Cipher is unable to encrypt the images properly if the image consists of large area covered with same color or gray level. But their suggested algorithm works for any images with different gray scale as well as color images.

In 2011, Tariq Shah et al [20] shows a criterion which analyze the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption applications. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S8 AES, SKIPJACK, and Xyi Sboxes.

In 2012, Somdip Dey [10] presents SD-EI technique for encrypt images which contains two stages: In first stage, each pixel is converted to its equivalent 8-bit binary number which equal to the length of password are rotated and then reversed. In second stage, extended Hill Cipher technique was applied which generate same password used in second stage of encryption to make system highly secure.

In 2012, Long Baoa et al. [11] demonstrate new image encryption scheme using the chaotic system. They reviles that the proposed image encryption scheme shows excellent encryption performance, high sensitivity to the security keys, and offer a sufficiently large key space to resist the brute attack.

In 2012, Anoop B N et al. [12] present a system of secure image transcoder which mainly focuses on multimedia applications like web browsing through mobile phones, in order to improve their delivery to client devices with wide range of communication. Their system based on CKBA encryption ensures end to end security.

In 2013, Praloy Shankar De et al. [13] try to make the focus on an algorithm of cryptography that was made by using methodologies which is old. DEDD Symmetric key cryptosystem is the new approach to symmetric key algorithm. By this method they suggested that they can doubly encrypt and doubly decrypt the message. It means the sender will generate the cipher text from the plain text twice. The receiver will also have to decrypt the ciphers for two times and then the communication between them will be completed. For generating the key, they will apply shifting technique.

III.EXISTING ENCRYPTION METHOD

A. SCAN based image encryption

The SCAN is a formal language based on two dimensional [16] spatial accessing methodologies which can represent and generate a large number of wide variety of scanning paths or space filling curves easily. There are a family of formal languages such as Simple SCAN, Extended SCAN, and Generalized SCAN, each of which can represent and generate a specific set of scanning paths. It is first employed for image encryption.

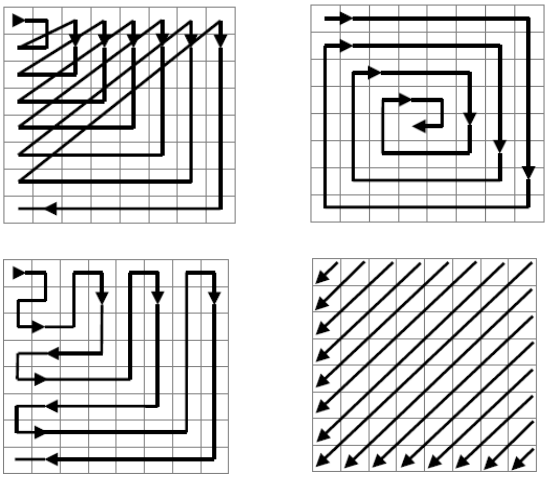

Fig. 2 SCAN pattern

The plain image is initially serialized to one dimensional data stream which is then described by the SCAN language [14][15]. Several scanning orders are expressed into the corresponding SCAN letters. Combinations of SCAN letters from different kinds of secret images. The SCAN string is served as an encryption key bound to a given 2D image array. The encryption procedure is to rearrange image into a final sequential representation. Each assembled secret image in process of SCAN string is combined by the insertion of additive noises at particular image points. Since no one except the intended user can obtain the correct SCAN combinations, the original image is therefore considered confidential.

B. Selective bit plane encryption

Intuitively, SE seems to be a good idea in any case since it is always desirable to reduce the computational demand involved in image processing applications. However, the security of such schemes is always lower as compared to full encryption. The only reasons to accept this drawback are significant savings in terms of processing time or power.

Therefore, the environment in which SE should be applied needs to be investigated thoroughly in order to decide whether its use is sensible or not.

Due to requirements of certain applications a loss of image quality may not be acceptable during transmission or storage (e.g., in medical applications because of reasons related to legal aspects and diagnosis accuracy [21]).

Lossless compression schemes need to be employed for such applications. We assume a target environment, where due to the low processing power of the involved hardware not even lossless compression and decompression of visual data is reasonable or possible (e.g. mobile clients).

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

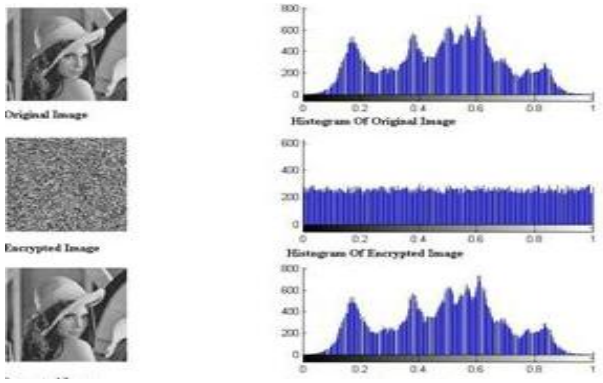

Fig.3 Example of Image Encryption

Additionally, due to the increasing bandwidth available at mobile communication channels, compression seems not to be mandatory in any case, which is especially true for lossless applications. The reason is that the data reduction of lossless compression schemes is much lower as compared to lossy ones making the respective application less profitable. Note also that the time demand for compression is significantly higher as the time demand for encryption for almost all high quality codecs and symmetrical ciphers (which is mostly due to the efficient cache use of block-based encryption).

C. Embedding image compression into encryption

The above mentioned schemes are devoted to the uncompressed image data. For compressed images, some special measures are required before strictly combining encryption and compression directly. A framework is proposed for fast encryption by entropy encoders such as Huffman coder. In entropy coding, the statistical model is used to decode the compressed bit stream. It is therefore suggested that multiple statistical models are used alternately in certain secret order to encode the input symbol stream [18]. Through security analyses, this scheme is proved to be applied effectively on both multiple Huffman coding tables of Huffman coder and multiple state indices of QM coder. However, it should be noted that the original image can be correctly reconstructed only if its input is identical to the output of the encoder. There is also a concern about codec dependence of such kind of scheme [19]. Nevertheless, the potential for integrating encryption with multimedia compression at a low computation is promised

D. Image encryption using chaotic map

Chaos signals are considered good for practical use because they have important characteristics such as they are highly sensitive to initial conditions and system parameters, they have pseudo-random property and non-periodicity as the chaotic signals usually noise-like, etc. Consequently, the combination of chaotic theory and cryptography forms an important field of information security. Chaos theory has been established by many different research areas, such as physics, mathematics, engineering, and biology [21]. Since last decade, many researchers have noticed that there exists the close relationship between chaos and cryptography [22].

Pareek et al. [23], point out an image encryption scheme which utilizing two chaotic logistic maps and an external key of 80-bit. The initial conditions for both logistic maps were obtained from the external secret key. The first logistic map was used to generate numbers in the range between 1 and 24. The authors showed that by modifying the initial condition of the second logistic map in such a way that its dynamics became more random.

Yen et al. [24] suggest an encryption method called BRIE based on chaotic logistic map. The basic principle of BRIE is bit recirculation of pixels, which is controlled by a chaotic pseudo random binary sequence. The secret key of BRIE consists of two integers and an initial condition of the logistic map.

Jiankun Hu et al [25] presented a novel pixel-based scrambling scheme to protect and secure way, the distribution of digital medical images. To provide an efficient encryption of a large volume of digital medical images, the proposed system uses simple pixel level XOR operation for image scrambling in an innovative way such that structural parameters of the encryption scheme have become a part of the cryptographic key. Two techniques for random number generation are discussed below.

i) Image Encryption Using Linear Congruential Generator

It generates two random number sequences based on linear congruential equation:

$Xn+1 = (aXn+c) \bmod m$

Where a – multiplier , m – modulus C –constant to be added

Then image permutation occurs by shuffling row, columns and pixel of image One sequence is used for row shuffling and another is used for column shuffling. A masking operation [26] is used after row and column shuffling by simple XOR operations between adjacent rows and columns.

ii) Image encryption using chaotic logistic map

It generated two random number sequences based on logistic map which is mathematical iterative system:

$Xn+1 = r*Xn*(1-Xn)$ ..... (3)

Where r is growth rate parameter.

By choosing appropriate seed value (Xn) and growth rate (r), linear equation is able to generate random number sequence [28] [26] [27]. One sequence is used for row shuffling, another for column shuffling. Pixel shuffling is done by taking both sequences together, same as scheme (A). A masking operation [29] is used after row and column shuffling by simple XOR operations between adjacent rows and columns.

IV. CONCLUSION

In the modern digital world, with the fast progression of data exchange in electronic way, information security is becoming more important in transmission as well as data storage. Because of widely using images in industrial purposes, it is important to protect the confidential image data from unauthorized access. This paper surveyed existing work on image encryption, and also provide general guide line about cryptography. Techniques describes in this paper that can provide highly security..

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

REFERENCES

[1] Behrouz A. Forouzan "Cryptography and Network Security"
[2] Garry C. Kessler, "An Overview of Cryptography", http://www.garykessler.net/library/crypto.html#intro
[3] "Practical Cryptography - HILL CIPHER", http://practicalcryptography.com/ciphers/hill-cipher/
[4] Vidit kumar Singh, "Hill Cipher–Essays-Vidschauhan", http://www.studymode.com/essays/Hill-Cipher-1592453.html
[5] Garry C. Kessler, "An Overview of Cryptography", http://www.garykessler.net/library/crypto.html#intro.
[6] Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Cho, Ha-Woo Lee and Soo-Joong Kim, "Multi-Level Image Encryption by Binary Phase XOR Operations", The 5th Pacific Rim Conference on Lasers and Electro-Optics, CLEO/Pacific Rim 2003, Taipei 106, Taiwan, 15-19 Dec. 2003.
[7] Li. Shujun, Li. Chengqing, C. Guanrong, Fellow., IEEE., Dan Zhang., and Nikolaos,G., Bourbakis Fellow., IEEE. "A general cryptanalysis of permutation-only multimedia encryption algorithms," 2004.
[8] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science,vol. 1, no. 1, p.127, 2006.
[9] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009, pp. 663 - 667.
[10] Somdip Dey, "SD-AI: A Cryptographic Technique to Encrypt Images", International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 26-28 June 2012, pp. 28 – 32.
[11] Long Bao, Yicong Zhou,C. L. Philip Chen," A New Chaotic System for Image Encryption", 2012 International Conference on System Science and Engineering June 30-July 2, 2012, Dalian, China.
[12] Anoop B N, Sudhish N George , Deepthi P P," Secure Image Transcoding technique using chaotic key based algorithm", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4 Issue-6 December-2012
[13] Praloy Shankar De, Prasenjit Maiti," DEDD Symmetric-Key Cryptosystem", International Journal of Advanced Computer Research (IJACR) ,Volume-3 Number-1 Issue-8 March-2013.
[14] Kachris, Christophoros. "Design and FPGA implementation of the SCAN encryption algorithm." PhD diss., Technical University of Crete, 2003.
[15] Chen,Chao-Shen, and Rong-Jian Chen." Image encryption and decryption using SCAN methodology" In Parallel and Distributed Computing, Applications and Technologies, Seventh International Conference on, pp.61-66 IEEE, 2006
[16] Maniccam S. S, Bour Bakis N. G," scan based lossless image compression and encryprition" , information intelligence and system, IEEE proceeding 1999 pages 490-499.
[17] M. Podesser, H.-P. Schmidt, A. Uhl, "Selective Bitplane Encryption Scheme for Secure Transmission of Image Data in Mobile Environments", Proc. of the 5th IEEE Nordic Signal Processing Symposium (NORSIG'02), Trondheim, Norway, October 2002.
[18] C.P. Wu, C.C. Kuo, "Design of Integrated Multimedia Compression and Encryption Systems" , IEEE Trans. Multimedia 7(5), pp. 828-839, 2005.
[19] Cheng, Howard, and Xiaobo Li. "Partial encryption of compressed images and videos." Signal Processing, IEEE Transactions on 48, no. 8, 2439-2451,2000.
[20] Tariq Shah, Iqtadar Hussain, Muhammad Asif Gondal , Hasan Mahmood, ‖ Statistical analysis of S-box in image encryption applications based on majority logic criterion ‖ , International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011
[21] Shubo Liu, Jing Sun, Zhengquan Xu,"An Improved Image Encryption Algorithm based on Chaotic System" Journal of Computers, Vol. 4, No. 11, 2009
[22] LIU Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin," Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation", International Journal of Computer Science and Network Security, VOL.8 No.1, 2008
[23] Vinod Patidar, N.K. Pareek , K.K. Sud ,"A new substitution–diffusion based image cipher using chaotic standard and logistic maps" "ELSEVIER , Communications in Nonlinear Science and Numerical Simulations 14, 3056–3075, 2009.
[24] J.C. Yen, J.I. Guo, "A new image encryption algorithm and its VLSI architecture", in: Proceedings of the IEEE workshop signal processing systems, pp. 430–437,1999.
[25] Hu, Jiankun, and Fengling Han. "A pixel-based scrambling scheme for digital medical images protection." Journal of Network and Computer Applications 32, no. 4. 2009
[26] G. Chen, Y.B. Mao, C.K. Chui, "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps", Chaos, Solitons and Fractals 12, pp. 749-761, 2004.
[27] Y.B. Mao, G. Chen, S.G. Lian, "A Novel Fast Image Encryption Scheme Based on the 3D Chaotic Baker Map", Int. J. Bifurcat. Chaos 14(10), pp. 3613-3624, 2004.
[28] C.E. Shannon, "Communication Theory of Secrecy System" , Bell Syst. Tech. J. 28, pp. 656-715, 1949.
[29] B. Furht, D. Socek, A.M. Eskicioglu, "Fundamentals of Multimedia Encryption Techniques", in B. Furht and D. Kirovski (Eds.), Multimedia Security Handbook, Ch. 3, CRC Press, 2005.

BIOGRAPHY

Ravindrakumar B. Prajapati receives his B.E. Degree in Electronics Engineering from The M. S. University, Vadodara, India in 2012. Also he started his M.E. in same university with specialization of Automatic Control and Robotics. He currently working as Assistant Professor at ITM Vocational University, Vadodara, India. During his master studies he has been involved in teaching to Undergraduate students. His main research areas include: image Processing, Control system, computer vision, and machine learning algorithms, soft computing Algorithms, pattern recognition, and inverse problems.