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

International Journal of Advanced Research in Computer and Communication Engineering
Volume 2, Issue 7, July 2013

A Review: Chaotic System with DES (Data Encryption Standard) Image Encryption Technique

Sonam Pathak[1], Rachana kamble[2]

Department of CSE, TIT Bhopal[1, 2]

Abstract: In any network communication like Internet, data encryption technique has been widely used to ensure information security. Each type of data has its own inherent characteristics. Therefore, different encryption techniques should be used to protect the confidential data from unauthorized access. There are other areas also where image encryption techniques are proposed for security purpose. In this paper we survey several image encryption techniques with their flaws and advantages; based on our survey we also suggested some future suggestions of image encryption, which may provide better security enhancement in the case of various types of images. We also discuss about the chaos based crypto system for better analysis with data encryption standard (DES) encryption.

Keywords – Image Encryption, Chaos, DES, Security Measures

1. INTRODUCTION

With the rapid developments of the communications industry, a great deal of concerns has been raised in the security of data transmitted or stored over open channels. Especially on the image data. A major challenge is to protect confidentiality for image data in digital distribution networks.

When the present determines the future, but the approximate present does not approximately determine the future is called chaos. Chaotic behavior can be observed in many natural systems, such as weather. These systems are capable of sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications.

According to [1] there are three basic methods of secured communication available, namely, cryptography, steganography and watermarking. Among these three, the first one, cryptography [2]-[4], deals with the development of techniques for converting information between intelligible and unintelligible forms during information exchange. Steganography [5]-[6], on the other hand, is a technique for hiding and extracting information to be conveyed using a carrier signal [1]. The third one, watermarking [7]-[8], is a means of developing proper techniques for hiding proprietary information in the perceptual data.

In [9] author suggest that the most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors [10]-[12]. So in order to achieve the higher correlation entropy among pixels and increasing the entropy value is an emerging research area.

In [13] the most significant problems, which affect the commerce of digital media, is how to protect copyright and ownership. The watermarking, 1 of the popular approaches consider ding as a tool for providing the copyright protection, is a technique based on embedding a specific mark or signature into the digital products. While several watermarking algorithms have been proposed [14] in this direction.

So in the subsequent section we discuss Data Encryption technique for image encryption. We also discuss the crucial aspects which are used in image encryption with their advantages and disadvantages. Finally based on the discussions we also suggest some future remark which may be fruitful in this direction.

The remaining of this paper is organized as follows. In Section 2 Literature Survey. In section 3 we discuss about the problem domain. Analysis is given in section 4 the conclusions and future directions are given in Section 5. Finally references are given.

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

International Journal of Advanced Research in Computer and Communication Engineering
Volume 2, Issue 7, July 2013

Data Encryption Standard (DES) [15]

Up until recently, the main standard for encrypting data was a symmetric algorithm known as the Data Encryption Standard (DES). DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. This is contrasted to a stream cipher in which only one bit at a time or sometimes small groups of bits such as a byte is encrypted.

The algorithm is designed to encipher and decipher blocks of data consisting of 64 bits under control of a 64-bit key. Deciphering must be accomplished by using the same key as for enciphering, but with the schedule of addressing the key bits altered so that the deciphering process is the reverse of the enciphering process. A block to be enciphered is subjected to an initial permutation IP, then to a complex key-dependent computation and finally to a permutation which is the inverse of the initial permutation IP^{-1}. The key-dependent computation can be simply defined in terms of a function *f*, called the cipher function, and a function KS, called the key schedule. A description of the computation is given first, along with details as to how the algorithm is used for encipherment. Next, the use of the algorithm for decipherment is described. Finally, a definition of the cipher function *f* is given in terms of primitive functions which are called the selection functions S_i and the permutation function P. The following notation is convenient: Given two blocks L and R of bits, LR denotes the block consisting of the bits of L followed by the bits of R. Since concatenation is associative, $B_1B_2...B_8$, for example, denotes the block consisting of the bits of B_1 followed by the bits of B2...followed by the bits of B8.

Blocks are composed of bits numbered from left to right, i.e., the left most bit of a block is bit one.

The computation which uses the permuted input block as its input to produce the pre output block consists, but for a final interchange of blocks, of 16 iterations of a calculation that is described below in terms of the cipher function *f* which operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits.

Let the 64 bits of the input block to an iteration consist of a 32 bit block L followed by a 32 bit block R. Using the notation defined in the introduction, the input block is then LR.

Let K be a block of 48 bits chosen from the 64-bit key. Then the output L'R' of iteration with input LR is defined by:

(1) L' = R
R' = L(+)f(R,K)

where (+) denotes bit-by-bit addition modulo 2.

As remarked before, the input of the first iteration of the calculation is the permuted input block. If L'R' is the output of the 16th iteration then R'L' is the pre output block. At each iteration a different block K of key bits is chosen from the 64-bit key designated by KEY.

With more notations we can describe the iterations of the computation in more detail. Let KS be a function which takes an integer *n* in the range from 1 to 16 and a 64-bit block KEY as input and yields as output a 48-bit block K_n which is a permuted selection of bits from KEY. That is

(2) $K_n = KS(n,KEY)$

with K_n determined by the bits in 48 distinct bit positions of KEY. KS is called the key schedule because the block K used in the *n*'th iteration of (1) is the block K_n determined by (2).

As before, let the permuted input block be LR. Finally, let $L_{()}$ and $R_{()}$ be respectively L and R and let Ln and Rn be respectively L' and R' of (1) when L and R are respectively L_{n-1} and R_{n-1} and K is K_n; that is, when *n* is in the range from 1 to 16,

(3) $L_n = R_{n-1}$
$R_nn = L_{n-1}(+)f(R_{n-1},K_n)$

The preoutput block is then $R_{16}L_{16}$.

The key schedule KS of the algorithm is described in detail in the Appendix. The key schedule produces the 16 K_n which are required for the algorithm.

Deciphering

The permutation IP^{-1} applied to the preoutput block is the inverse of the initial permutation IP applied to the input. Further, from (1) it follows that:

(4) R = L'
L = R' (+) f(L',K)

Consequently, to decipher it is only necessary to apply the very same algorithm to an enciphered message block, taking care that at each iteration of the computation the same block of key bits K is used during decipherment as was used during the encipherment of the block. Using the notation of the previous section, this can be expressed by the equations:

(5) $R_{n-1} = L_n$
$L_{n-1} = R_n$ (+) $f(L_n,K_n)$

where now $R_{16}L_{16}$ is the permuted input block for the deciphering calculation and $L_{()}$ and $R_{()}$ is the preoutput block. That is, for the decipherment calculation with $R_{16}L_{16}$ as the permuted input, K_{16} is used in the first iteration, K_{15} in the second, and so on, with K_1 used in the 16th iteration.

II. LITERATURE SURVEY

In 2003, Sinha A. and Singh K. [16] proposed a technique to encrypt an image for secure transmission using the digital signature of the image. Digital signatures enable the recipient of a message to authenticate the sender of a message and verify that the message is intact.

In 2004, Shujun Li et al. [17] have pointed out that all permutation-only image ciphers were insecure against known/chosen-plaintext attacks. In conclusion, they suggested that secret permutations have to be combined with other encryption techniques to design highly secured images.

In 2005, Zhi-Hong Guan et al. [18] have presented a new image encryption scheme, in which shuffling the positions

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

International Journal of Advanced Research in Computer and Communication Engineering
Volume 2, Issue 7, July 2013

and changing the grey values of image pixels are combined to confuse the relationship between the cipher image and the plain image.

In 2006, Mitra A et al. [1] have proposed a random combinational image encryption approach with bit, pixel and block permutations. The main idea behind their work is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. This perceivable information can be reduced by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. From the results, it is observed that the permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation.

In 2013, Praloy Shankar De et al. [19] attempt has been made to focus on an algorithm of cryptography that was made by using old methodologies. DEDD Symmetric-key cryptosystem is the new approach to symmetric key algorithm. By this method 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 take the message length in first encryption and in second encryption they will apply shifting technique.

In 2013, Seetaiah Kilaru et al. [20] suggest that security is the main concern in any field. With the frequent attacks, it is a big challenge for the users to protect the digital images which are transmitting over internet. Singular Value Decomposition (SVD) [7] provides a solution up to a greater extent. Author suggests that by using the Wavelets, invisible watermark embed into the original watermark. The main focus concentrated on the wireless communications; hence it is important to consider some factors into consideration, they are size of an image and requirements of bandwidth. Keeping in view of all these parameters, compression and transmission should be done. The proposed algorithm by [20] uses the SVD method along with compression. The proposed algorithm is robust against all common attacks which exist in image processing field. Tests have been done and results are satisfactory in terms of imperceptibility and security.

In 2012, Long Baoa et al. [21] proposed chaotic system shows excellent chaotic behaviors. To demonstrate its application in image processing, a new image encryption scheme using the proposed chaotic system is also introduced. Computer simulation and security analysis demonstrate that the proposed image encryption scheme shows excellent encryption performance, high sensitivity to the security keys, and a sufficiently large key space to resist the brute attack. But in this paper random like nature of chaos is not considered.

III. PROBLEM DOMAIN

After discussing several research works we can come with some problem area in the traditional approaches which are following:

Traditional algorithm fails to work on the basis of double encryption and decryption. This can be achieved by the algorithm which is used in [19]. By this algorithm we can better secure the images or the data.

There is the need of DES, RSA algorithm to be used for image encryption and decryption. We can apply DES and RSA algorithm so that the size of key spaces can be increased and attacking by the brute force technique is weak.

- Large Key with high random sensitivity for key generation is needed.
- Entropy should be increases based on the pixels.
- The algorithm must support color histograms with logical key space.
- We can use steganography concept on image encryption to make it more complex to attack.

IV. ANALYSIS

After studying and observing several research works we compare the result discussions by their techniques, so that we identify the good and flaws presented in the previous research.

S. no	Approach	Information Accuracy	Information accuracy after Encryption
1	SPN structure [21]	Leena Image 7.5534	7.9669
2	SPN structure [21]	Circle Image 6.0408	7.9652
3	SPN structure [21]	Clock Image 6.7057	7.9667
4	PSNR Comparison [20]	Clown Image 39.43	Clown Image 32.52
5	PSNR Comparison [20]	Couple Image 39.57 9	Couple Image 30.69
6	Block Based Transformation [9] Proposed technique 30 × 30	0.0063	5.4402

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

International Journal of Advanced Research in Computer and Communication Engineering
Volume 2, Issue 7, July 2013

7	Block Based Transformation [9] Proposed technique 60 × 60	0.0049	5.5286
8	Block Based Transformation [9] Proposed technique 100 × 100	0.0044	5.5407

V. CONCLUSION AND FUTURE WORK

All of the above discussed techniques which are already proposed. We also discuss about the DES encryption techniques. Based on the above study we provide the following future directions which can be helpful in better detection:

1) We can use Powerful encryption technique like DES and RSA.
2) It can increase the size of key also, so that brute force attack is not easy.
3) Random password initialization also helps it in the security improvement.
4) Increasing the block size can improve the security.
5) Chaos-based ciphers should not be susceptible to traditional differential and
linear cryptanalysis attacks so hybridization is the better possibility.

REFERENCES

[1] 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.
[2] A. J. Elbirt and C. Paar, "An Instruction-Level Distributed Processor for Symmetric-Key Cryptography," IEEE Trans. Parallel and distributed systems, vol. 16, no. 5, pp. 468-480, May 2005.
[3] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.
[4] W. Stallings, Cryptography and Network Security. Englewood Cliffs,NJ: Prentice Hall, 2003.
[5] E. Besdok, "Hiding information in multispectral spatial images," Int. J.Electron. Commun. (AEU) 59, pp. 15-24, 2005.
[6] S. Trivedi and R. Chandramouli, "Secret Key Estimation in Sequential Steganography," IEEE Trans. Signal Processing, vol. 53, no. 2, pp. 746-757, Feb. 2005.
[7] Y. Wu, "On the Security of an SVD-Based Ownership Watermarking,"IEEE Trans. Multimedia, vol. 7, no. 4, pp. 624-627, Aug. 2005.
[8] Y. T. Wu and F. Y. Shih, "An adjusted-purpose digital watermarking technique," Pattern Recognition 37, pp. 2349-2359, 2004.
[9] Mohammad Ali Bani Younes and Aman Jantan," Image Encryption Using Block-Based Transformation Algorithm", IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03.
[10] S. P. Nana'vati., P. K. panigrahi. "Wavelets:applications to image compression- I,". Joined of the scientific and engineering computing, vol. 9, no. 3, 2004, pp. 4- 10.
[11] c. Ratael, gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.
[12] AL. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo,"Video over IP using standard-compatible multiple description coding," Journal of Zhejiang University- Science A, vol. 7, no. 5 ,2006, pp. 668- 676.
[13] Neha Chauhan, Akhilesh A. Waoo, P. S. Patheja," Attack Detection in Watermarked Images with PSNR and RGB Intensity", International Journal of Advanced Computer Research (IJACR) Volume-3 Number-1 Issue-9 March-2013.
[14] G. Voyatzis, N. Nikolaidis and I. Pitas, "Digital watermarking: An overview", EUSIPCO, vol. 1, pp. 9-12, 1998.
[15] Ms. Shikha Joshi, Ms. Pallavi Jain," A Secure Data Sharing and Communication with Multiple Cloud Environments with Java API", International Journal of Advanced Computer Research (IJACR)
Volume 2 Number 2 June 2012.
[16] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218, no. 4, 2003.
[17] 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.
[18] G. Zhi-Hong, H. Fangjun, and G. Wen ie , " Ch aos - based image encryption algorithm,"Department of Electrical and computer Engineering, University of Waterloo, ON N2L 3G1, Canada. Published by: Elsevier, 2005, pp. 153-157.
[19] Praloy Shankar De, Prasenjit Maiti," DEDD Symmetric-Key Cryptosystem", International Journal of Advanced Computer Research (IJACR) ,Volume-3 Number-1 Issue-8 March-2013.
[20] Seetaiah Kilaru, Yojana Kanukuntla, K B S Chary," An effective algorithm for Image security based on Compression and Decomposition method", International Journal of Advanced Computer Research (ISSN (IJACR) Volume-3 Number-1 Issue-8 March-2013.
[21] 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.