International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB

Jai Singh[†]*, Kanak Lata[†] and Javed Ashraf[‡]

[†]Dept. of Electronics & Comm., Maharshi Dayanand University, Rohtak, Haryana, India
[‡]Dept. of Electronics & Comm., Jamia Milia Islamia University, New Delhi, India

Accepted 20 Feb 2015, Available online 25 Feb 2015, **Vol.5, No.1 (Feb 2015)**

Abstract

Any communication in the language that you and I speak—that is the human language, takes the form of plain text or clear text. That is, a message in plain text can be understood by anybody knowing the language as long as the message is not codified in any manner. So, now we have to use coding scheme to ensure that information is hidden from anyone for whom it is not intended, even those who can see the coded data. Cryptography is the art of achieving security by encoding messages to make them non-readable. Cryptography is the practice and study of hiding information. In modern times cryptography is considered a branch of both mathematics and computer science and is affiliated closely with information theory, computer security and engineering. Cryptography is used in applications present in technologically advanced societies; examples include the security of ATM cards, computer passwords and electronic commerce, which all depend on cryptography. There are two basic types of cryptography: Symmetric Key and Asymmetric Key. Symmetric key algorithms are the quickest and most commonly used type of encryption. Here, a single key is used for both encryption and decryption. There are few well-known symmetric key algorithms i.e. DES, RC2, RC4, IDEA etc. In this Project digital images encrypted and decrypted by using symmetric key cryptography using MATLAB.

Keywords: *DES, Cryptograph, Symmetric Key, Encryption, Decryption, Cipher, Encipher, Image Encryption.*

1. Introduction

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public key (or asymmetric) cryptography, and hash functions. The rapid continuous increase in exchange of multimedia data over protected and unprotected networks such as the worldwide available internet and local networks such as shared networks and local area networks etc has encouraged activities such as unauthorized access, illegal usage, disruption, alteration of transmitted and stored data. This widely spread use of digital media over the internet such as on social media, won cloud storage systems etc and over other communication medium such as satellite communication systems have increased as applications and need for systems to meet current and future demands evolved over the years. Security concerns with regards to such data transmission and storage has been a major concern of both the transmitters and receivers and hence the security of critical cyber and physical infrastructures as well as their underlying computing and communication architectures and systems becomes a very crucial priority of every institution.

Cryptography is the fundamental platform in which modern information security, which involves the use of advanced mathematical approaches in solving hard cryptographic issues, has gained its grounds in the digital world. This has evolved from classical symmetric, in which shifting keys are normally used as well as substitution methods, ciphers to modern public key exchange cryptosystems, which aims to make cryptanalysis a difficult approach to deciphering ciphers, eg. RSA, ElGamal, elliptic curve, Diffie-Hellman key exchange, and they are used in digital signature algorithms and now cutting edge works such as the quantum cryptography.

2. Related Work

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing.

*Corresponding author: **Jai Singh**

Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time, and implement some form of feedback mechanism so that the key is constantly changing.

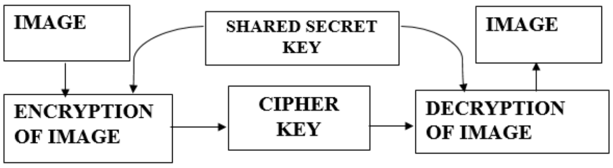


Fig.1 Symmetric Key Cryptography Process

In above fig.1 Blocks are given which is implemented step by step for image encryption by using symmetric key cryptography for encryption and decryption.

2.1 Cryptography Terminology

a) **Plaintext**: The original intelligible message.
b) **Cipher text**: The transformed message.
c) **Cipher**: An algorithm for transforming an intelligible message to unintelligible by transposition.
d) **Key**: Some critical information used by the cipher, known only to the sender & receiver.
e) **Encipher**: (Encode) the process of converting plaintext to cipher text using a cipher and a key.
f) **Decipher**: (Decode) the process of converting cipher text back into plaintext using a cipher & key.
g) **Cryptanalysis**: The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called code breaking
h) **Cryptology**: Both cryptography and cryptanalysis
i) **Code**: an algorithm for transforming an intelligible message into an unintelligible one using codes.
j) **Hash algorithm**: Is an algorithm that converts text string into a string of fixed length.
k) **Secret Key Cryptography (SKC)**: Uses a single key for both encryption and decryption.
l) **Public Key Cryptography (PKC)**: Uses one key for encryption and another for decryption.
m) **Pretty Good Privacy (PGP)**: PGP is a hybrid cryptosystem.
n) **Public Key Infrastructure (PKI)**: PKI feature is Certificate authority.

3. Image Encryption

This paper based on Image Encryption & Decryption. The user will give an input and encryption factor. The image will be converted to an encrypted image file. This image is not understandable by any one.

When the receiver will receive the encrypted file he will decrypt it so he will get the original file. We have used a simple GUI for our cryptosystem. We have used three push buttons in our GUI representing

1. Input Image Select
2. Encrypt Image
3. Decrypt Image

Image encryption approaches fall into two broad categories: spatial domain methods and frequency domain methods. The term spatial domain refers to the image plane itself, and approaches in this category are based on direct manipulation of pixels in an image. In these algorithms, the general encryption usually destroys the correlation among pixels and thus makes the encrypted images incompressible. Frequency domain processing techniques are based on modifying the Fourier transform of an image. The Fourier transform can be reconstructed (recovered) completely via an inverse process with no loss of information. This is one of the most important characteristics of this representation because it allows us to work in the Fourier domain and then return to the original domain without losing any information. Encryption techniques based on various combinations of methods from these two categories are not unusual. In this paper we present a novel image encryption scheme which employs magnitude and phase manipulation using Differential Evolution (DE) approach. It deployed the concept of keyed discrete Fourier transform (DFT) followed by DE operations for encryption purpose.

Firstly two dimensional (2-D) keyed discrete Fourier transform is carried out on the original image to be encrypted. Secondly crossover is performed between two components of the encrypted image, which are selected based on Linear Feedback Shift Register (LFSR) index generator. Similarly, keyed mutation is performed on the real parts of a certain components selected based on LFSR index generator. The LFSR index generator initializes it seed with the shared secret key to ensure the security of the resulting indices. The process shuffles the positions of image pixels. A new image encryption scheme based on the DE approach is developed which is composed with a simple diffusion mechanism. The deciphering process is an invertible process using the same key. The proposed method, dealing with private key cryptosystem, works in the frequency domain. The basis for the proposed method is that the encrypted image is obtained by magnitude and phase manipulation of the original image using the secret key. The original image magnitude and phase can be uniquely retrieved from the encrypted image if and only if the key is known. The resulting encrypted image is found to be fully distorted, resulting in increasing the robustness of the proposed work.

4. Data Encryption Standard Technique

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits, and it is always quoted as such.

The key is nominally stored or transmitted as 8 bytes, each with odd parity. According to ANSI X3.92-1981 (Now, known as ANSI INCITS 92-1981), One bit in each 8-bit byte of the KEY may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16, 64 are for use in ensuring that each byte is of odd parity.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in a mode of operation. FIPS-81 specifies several modes for use with DES. Further comments on the usage of DES are contained in FIPS-74.

Decryption uses the same structure as encryption but with the keys used in reverse order. (This has the advantage that the same hardware or software can be used in both directions.)

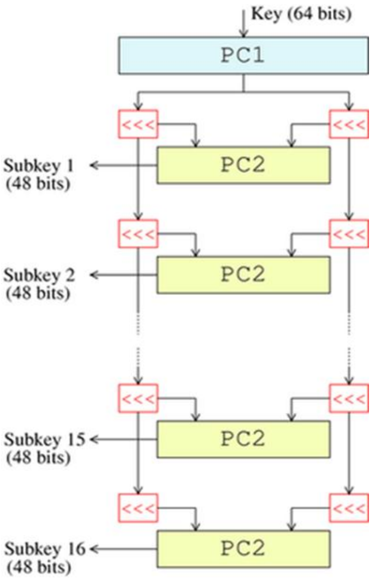


Fig. 2 Key Schedule for DES

The key schedule for encryption — the algorithm which generates the subkeys. Initially, 56 bits of the key are selected from the initial 64 by Permuted Choice 1 (PC-1) — the remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately. In successive rounds, both halves are rotated left by one and two bits (specified for each round), and then 48 subkey bits are selected by Permuted Choice 2 (PC-2) — 24 bits from the left half, and 24 from the right. The rotations (denoted by <<< in the diagram) mean that a different set of bits is used in each subkey; each bit is used in approximately 14 out of the 16 subkeys.

The key schedule for decryption is similar — the subkeys are in reverse order compared to encryption. Apart from that change, the process is the same as for encryption. The same 28 bits are passed to all rotation boxes.

5. Simulation Work on Matlab

Now explanation of Matlab Work for Encryption & Decryption of image with symmetric key.

STEP 1: Open MATLAB software & WRITE the CODE FOR ENCRYPTION & DECRYPTION
STEP 2: CLICK ON RUN in MATLAB Software on the middle Top view.
STEP 3: After RUN a Tab open for image select which we have to Encrypt.
STEP 4: After selection of image we have to go Command Window for Selection Key.
STEP 5: After selection of Key **(6)** it shows the input image (original) & create encrypt image of input image.

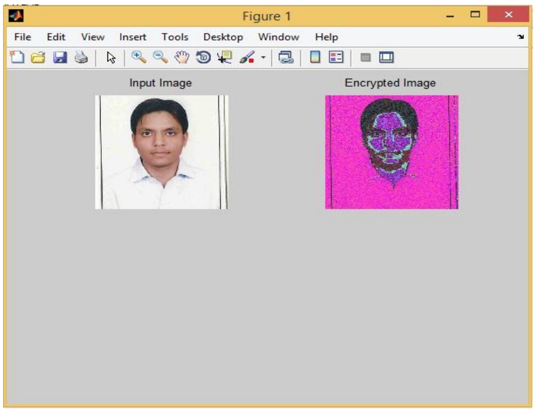


Fig.3 Input original image and encrypted image

STEP 6: Now for Decryption it will ask again KEY.
STEP 7: Enter the Key which is same is (6) for Decryption.
Note: In Symmetric Key always we use same key so here Numeric key (6) is used for both Encryption & Decryption.

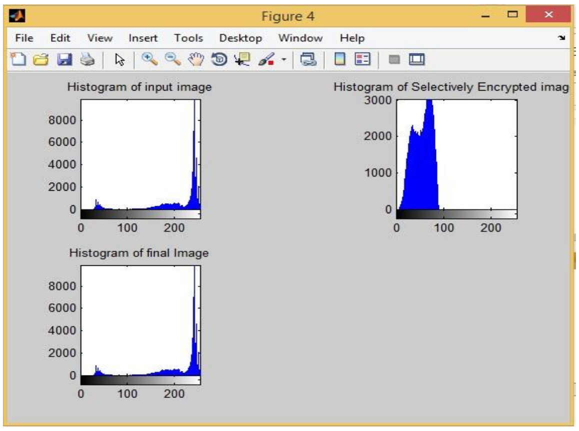


Fig.4 Histogram of input image & Encrypted Image

STEP 8: It shows the Histogram also for each image for input image, encrypt image and decrypt image.
We see histogram in which input image histogram and final decrypt image histogram is same.

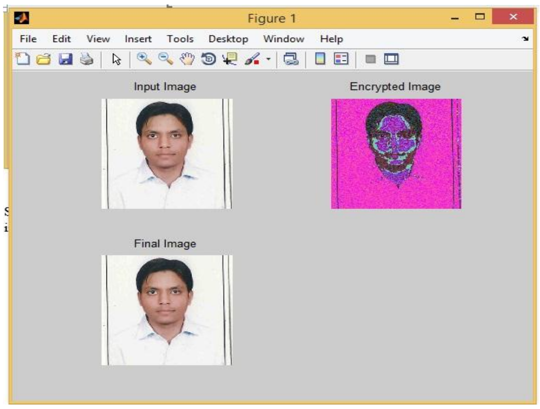
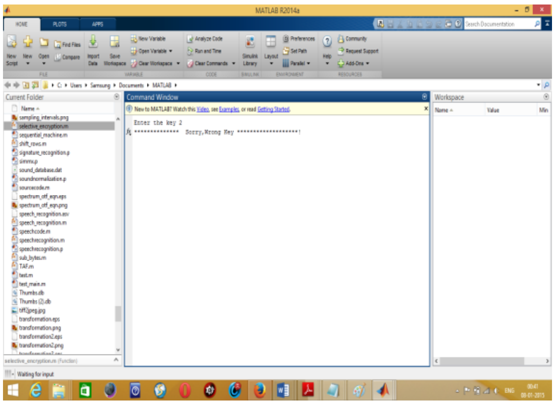


Fig.5 Final Decrypted image

STEP 9: see histogram of image fig.4 and compare and via histogram we understood our image is in original form successfully decrypted.

STEP 10: Finally we also get final image as input image after Decryption which is shows in fig. 5.

But further we also check if we select wrong key for decryption then what happened,
Again all process is same from STEP 2 to STEP 6 but in STEP 7 if we enter wrong key then message will show on command window is sorry, wrong key, shows in fig.6



```
Enter the key 2
*************  Sorry,Wrong Key *****************!
```

Fig.6 Message of Wrong Key

Conclusion

Code successfully work for Encryption & Decryption of Image with using of Symmetric Key with histogram Analysis we found if we select same key in Symmetric Method for both encryption and decryption image it shows the original final image, but we Key is different when we decrypt the image it's shows wrong Key.

Further we can analysis more images for encryption and decryption, in IT we have Data collection in the form of Digital Information which is in the form of textual it can also be required to make sure for encryption from hackers and resolution, graphics and pixels of images also analysis how much they were take time to elapsed for output. Symmetric key always use for large message which is good for as per using single key.

References

Kumar, M.; Hensman, (June 2013) A., Robust digital video watermarking using reversible data hiding and visual cryptography, *Signals and Systems Conference* (ISSC 2013), 24th IET Irish , vol., no., pp.1,6, 20-21 doi: 10.1049/ic.2013.0051

Fouad, M.; El Saddik, A.; Jiying Zhao; Petriu, E., (2011) Combining cryptography and watermarking to secure revocable iris templates, *Instrumentation and Measurement Technology Conference* (I2MTC), IEEE , vol., no., pp.1,4, 10-12 May 2011doi: 10.1109/IMTC.2011.5944015

Bhargava, N.; Sharma, M.M.; Garhwal, A.S.; Mathuria, M., (2012), Digital image authentication system based on digital watermarking, Radar, Communication and Computing *ICRCC*, 2012 International Conference on, vol., no., pp.185,189, doi:10.1109/ICRCC.2012.6450573

Shing-Chi Cheung, Dickson K. W. Chiu, and Cedric Ho. (2008). The use of digital watermarking for intelligence multimedia document distribution. J. Theor. Appl. Electron. Commer. Res. 3, 3 (December 2008), 103-118.

Stelvio Cimato, James Ching-Nung Yang, and Chih-Cheng Wu. (2012). Visual cryptography based watermarking: definition and meaning. In Proceedings of the 11th *International conference on Digital Forensics and Watermaking* (IWDW'12), Yun Q. Shi, Hyoung-Joong Kim, and Fernando Pérez-González (Eds.). Springer-Verlag, Berlin, Heidelberg, 435-448. DOI=10.1007/978-3-642-40099-5_36 http://dx.doi.org/10.1007/978-3-642-40099-5_36

I-Kuan Kong and Chi-Man Pun. (2008). Digital Image Watermarking with Blind Detection for Copyright Verification. In Proceedings of the 2008 *Congress on Image and Signal Processing*, Vol. 1 - Volume 01 (CISP '08), Vol. 1. IEEE Computer Society, Washington, DC, USA, 504-508. DOI=10.1109/CISP.2008.546 http://dx.doi.org/ 10.1109/CISP.2008.546

Huiping Guo. (2003). Digital Image Watermarking for Ownership Verification. Ph.D. Dissertation. University of Ottawa, Ottawa, Ont., Canada, Canada. Advisor(s) Nicolas Georganas. AAINQ85364.

Huaqing Liang, Hongdong Yin, and Xinxin Niu. (2009). A Robust Digital Watermarking Scheme and Its Application in Certificate Verification. In *Proceedings of the 2009 International Conference on Measuring Technology and Mechatronics Automation* - Volume 01 (ICMTMA '09), Vol. 1. IEEE Computer Society, Washington, DC, USA, 410-413. DOI=10.1109/ICMTMA.2009.295 http://dx.doi.org/10.1109/ICMTMA.2009.295

Singh, T.R.; Singh, K.M.; Roy, S., (2012) Robust video watermarking scheme based on visual cryptography, *Information and Communication Technologies* (WICT), World Congress on, vol., no., pp.872,877, Oct. 30 2012-Nov. 2 2012 doi: 10.1109/WICT.2012.6409198

Cox, J.; Miller, M. L.; Bloom, J. A.; Fridrich J. & Kalker T. (2008). Digital Watermarking and Steganography, *Morgan Kaufmann Pub., Elsevier Inc.*

C. C. Chang, P. Tsai and C. C. Lin, (2005) SVD-based digital image watermarking image scheme, *Pattern Recognition Letters*, vol.26, pp. 1577-1586.

A. A. Mohammad, A. Alhaj and S. Shaltaf,(2008) An improved SVD-based watermarking scheme for protecting rightful ownership, *Signal Processing*, vol. 88, pp. 2158-2180.

K. L. Chung, W. N. Yang, Y. H. Huang, S. T. Wu, and Y .C. Hsu, (2007) On SVD-based watermarking algorithm, *Applied Mathematics & Computation*, vol. 188, pp. 54-57, 2007.

Hsiang-Cheh Huang, C.-M.C.a.J.-S.P., (2008). The optimized copyright protection system with genetic watermarking. *A Fusion of Foundations, Methodologies and Applications*.

P. S. Murty, K. S. Dileep and P. R. Kumar, (2013) A Semi Blind Self Reference Image Watermarking in Discrete Cosine Transform using Singular Value Decomposition, *International Journal of Computer Applications*, vol. 62, issue 13, pp. 29-36