A Comparative Literature Survey On Various Image Encryption Standards

Ms. Ankita P. Baheti
PG Student, TIT

Prof. Lokesh Singh
Asst. Professor, TIT

Prof. Asif Ullah Khan
Director, TIT

Abstract

As multimedia applications are used increasingly, security becomes an important issue of communication and storage of images. Encryption is one of the ways to ensure high security. Images are used in many fields such as medical science, military; they are stored or transfer through network, security of such image data is important. Text encryption algorithms which have been already developed are not suitable for the image encryption, because image containing large amount of data means it contains number of pixels. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image. In this paper survey of basic encryption standards, symmetric as well as other image encryption techniques has been discussed.

1. Introduction

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes the way to hide information in storage or transit. However in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

- Confidentiality: The information should be kept secret.
- Integrity: The information should not get altered in storage or transit.
- Non-repudiation: The intentions of sender or receiver should not be changed at later stage.
- Authentication: The sender and receiver should confirm each other.
- Key Management: Distribution of secret keys for encryption and decryption.

2. Basic Encryption Techniques

Basically cryptographers divide the encryption algorithms depending on the type of transformation and the keys. Some algorithms require prior agreement on secret key irrespective of the normal communication protocol. We describe a brief survey of such algorithms and their methods which they use in encryption and decryption of the data.

Secret –key cryptosystem

These algorithms encrypt and decrypt messages with a key in such a way that it is difficult to decrypt without the key. Because the encryption and decryption keys in a secret-key cryptosystem are the same, such systems are often called symmetric in the literature. Most secret-key cryptosystems operate on messages one block at a time; a block may be 64 bits long, and the keys are usually short, say, 56 bits long. Ideally, an attacker's only approach is trial and error. Secret-key cryptosystems provide confidentiality and key management to parties who have previously agreed on a secret key. The Data Encryption Standard (DES)[25] is the primary standard. Published in 1977 and recently affirmed for a fourth five-year period, DES defines the Data Encryption Algorithm (DEA)[21]. It also specifies how to implement DEA: in hardware. Despite much controversy about the nature of DEA-the government never revealed its design criteria-the algorithm seems to be quite secure, as far as 56-bit algorithms go. It resists powerful attacks that have broken other systems.[18] Secret-key cryptosystems are rarely standardized; some standards bodies explicitly omit them from their scope. One of the few other candidates is RC4, a fast secret-key cryptosystem with variable-length keys.[22] RC4 is adopted in the cellular digital packet data (CDPD)[18] specifications."

Table 1. Encryption algorithm classes and their properties

Class	C	OA	I	KM	Prior
Secret-key cryptosystems	Yes	No	No	Yes	Yes
Public-key cryptosystems	Yes	No	No	Yes	No
Digital signature schemes	No	Yes	Yes	No	No
Key-agreement algorithms	Yes	Optional	No	Yes	No
Cryptographic hash functions	No	No	Yes	No	No
Authentication codes	No	Yes	Yes	No	Yes

C indicates confidentiality; OA, origin authentication; I, integrity; KM, key management.
Prior requires that parties first agree on a secret key.

Public-key cryptosystem

These algorithms encrypt and decrypt messages with two different keys in such a way that it is difficult to decrypt without the decryption key. The encryption key can be published without compromising security. And is called the public key for this reason; the decryption key is called the private key. Because the encryption and decryption keys in a public-key cryptosystem differ, such systems are often called asymmetric in the literature. The idea comes from Diffie and Hellman [28]. Public-key cryptosystems provide confidentiality and key management. They can be as secure as or more secure than secret-key cryptosystems, but they are generally slower. Their main advantage is that, since the encryption key can be published, parties need not first agree on a secret key. They are often combined with secret-key cryptosystems to gain the benefits of both: speed without prior secrets.

Digital signature schemes

This scheme "sign" messages and verify the resulting signature with two different keys in such a way that it is difficult to sign without the signing key. Similar to public-key cryptosystems, the verification key can be published without compromising security, and is called the public key; the signing key is called the private key. Digital signature schemes provide integrity and origin authentication. Like public-key cryptosystems, they do not require that parties first agree on a secret key, and they are generally somewhat slower than, for instance, secret-key cryptosystems and cryptographic hash functions. They are often combined with hash functions to gain the benefits of both. Public-key cryptosystems and digital signature schemes are closely related. In so-called reversible cryptography, signing in a digital signature scheme is the same as decryption in a public- key cryptosystem, while verification is the same as encryption. In irreversible cryptography, the relationships do not hold, although a given public/private-key pair may work in both a digital signature scheme and a public-key cryptosystem. There is no primary standard digital signature scheme, but two main efforts are in progress. One involves RSA, which is proposed by the US National Institute of Standards and Technology (NIST). [23, 20]

Key-agreement algorithms

These algorithms manage keys through an exchange of messages derived from private values that are not shared. The result of the exchange is that parties agree on a secret key. It is difficult to determine the secret key from the exchanged messages without the private values from which they are derived. Key-agreement algorithms are sometimes called key exchange algorithms in the literature. Key-agreement algorithms provide confidentiality and key management, and in some cases origin authentication. They do not require that parties first agree on a secret key. As with public-key cryptosystems, no primary standard key-agreement algorithm exists. Many consider an algorithm invented by Diffie and Hellman,[28] usually called Diffie-Hellman, the de facto standard here. [24, 19]

Cryptographic hash functions

These functions diminish a message of arbitrary length to a short code so that it is difficult to find a message with a given hash code, and in some cases also to find two messages with the same hash code. There is no key. Hash functions are also called message digests and modification recognition codes in the literature. A hash code is typically 128 or 160 bits long. Ideally, an attacker's only use the brute force attack, which amounts to 212* trials to find a message with a given hash code (for a 128-bit hash), and 2M trials to find two messages with the same hash code. Hash functions are generally quite fast. They provide message reliability to parties knowing a message's hash code. They are often combined with digital signature schemes, as noted earlier.[20]

Authentication codes

These codes reduce a message of arbitrary length to a short code under a secret key *so* that it is difficult, without the key, to compute the authentication code, or to find a new message with a given authentication code. Authentication codes provide message integrity and origin secret key. The message itself need not be encrypted. An authentication code is typically 32 or 64 bits long, and the keys are 56 bits long. Ideally, an attacker's only approach is trial and error on the keys; arbitrary message modifications have some

probability of success, but the attacker cannot check for success without the help of the real user. Authentication codes, like hash functions, are generally quite fast.

3. Symmetric Key Algorithms

Cryptography algorithms play an important role in information security. They can be divided into Symmetric and Asymmetric key cryptography [5]. In Symmetric key encryption only one key is used to encrypt and decrypt data. The key should be circulated before transmission between two parties. Key plays an important role in encryption and decryption. If a weak key is used in the algorithm then easily data can be decrypted. The size of the key determines the strength of Symmetric key encryption. Symmetric algorithms are of two types: block ciphers and stream ciphers. The block ciphers are operating on data in groups or blocks. .Examples are of Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Blowfish. Stream ciphers are operating on a single bit at a time. RC4 is stream cipher algorithm. Encryption algorithms consume significant amount of computing resources such as battery power, CPU time, etc. Asymmetric key (or public key) encryption is used to solve the problem of key distribution [2]. In Asymmetric key encryption, two keys are used; private keys and public keys. Public key is used for encryption and private key is used for decryption (e.g Digital Signatures). Public key is known to the public and private key is known only to the user. Prior to transmission there is no need for distributing them. Asymmetric encryption techniques are near to 1000 times slower than Symmetric techniques, since they require more computational processing power.

Data Encryption Standards

DES is a block encryption algorithm. It was the first encryption standard published by NIST (National Institute of Standards and Technology) in 1976 [4,3].It is a symmetric algorithm, means same key is used for encryption and decryption .It uses one 64-bit key. Out of 64 bits, 56 bits make up the independent key, which determine the exact cryptography transformation; 8 bits are used for error detection.DES. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are applied in reverse order. The output is a 64-bit block of cipher text. Many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher key.

Table 2. Comparison of DES, 3DES, AES and Blowfish algorithm

	Symmetric Encryption Algorithms			
	DES	*TDES*	*AES*	*BLOWFISH*
Block Size	64 bit	64 bit	128 bit	64 bit
Key size	56 bit	168 bit	128,192, 256 bit	32-448 bit
Created By	IBM in 1975	IBM in 1978	Joan Daeman in 1998	Bruce Schneier in 1998
Algorithm Structure	Fiestel Network	Fiestel Network	Substitution Permutation Network	Fiestel Network
Rounds	16	48	9,11,13	16
Attacks	Brute Force Attack	Theoretically possible	Side Channel Attacks	Not Yet

Triple DES

Triple DES is an enhancement of Data Encryption Standard [1]. It uses 64 bit block size with 192 bits of key size [6]. The encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. Triple DES is slower than other block cipher methods. The following expression is used for encryption purpose.

$$C(t) = Ek1\ (Dk2\ (Ek3\ (t)))$$

Advanced Encryption Standards

Advanced Encryption Standard (AES) also known as the Rijndael algorithm is a symmetric block cipher [2]. It was recognized that DES was not secure because of advancement in computer processing power. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies [5]. It can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts the data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices [3]. AES has been tested for many security applications.

Each processing round involves four steps:

- Substitute bytes – Uses an S-box to perform a byte by byte substitution of the block,
- Shift rows – A simple permutation,
- Mix column – A substitution method where data in each column from the shift row step is multiplied
- by the algorithm's matrix and
- Add round key – The key for the processing round is XORed with the data.

Blowfish

It is one of the most public domain encryption algorithms [2]. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length. It takes a variable-length key from 32 bits to 448 bits. Blowfish has variants of 14 rounds or less [3]. Blowfish is a very secure cipher but it is has been replaced by Twofish and Rijndael due to its small 64 bit block size. Blowfish is one of the fastest block ciphers which has developed to date. Slowness kept Blowfish from being used in some applications. Blowfish was created to allow anyone to use encryption free of patents and copyrights. Blowfish has remained in the public domain to this day. No attack is known to be successful against it, though it suffers from weak keys problem.

4. Other Image Encryption Techniques

Modified AES

In Modified-AES the block length and the key length are specified according to AES specification: three key length alternatives 128, 192, or 256 bits and block length of 128 bits. We assume a key length of 128 bits, which is most commonly implemented. In Modified-AES encryption and decryption process resembles to that of AES, in account of number of rounds, data and key size. The round function consists of four stages. To overcome the problem of high calculation we skip the Mixcolumn step and add the permutation. Mixcolumn gives better security but it takes large calculation that makes the encryption algorithm slow [17]. The other three junctures remain unbothered as it is in the AES. A single 128-bit block is the input to the encryption and decryption algorithms. This block is a 4×4 square matrix consisting of bytes. This block is copied into the state array. The state array is modified at each stage of encryption or decryption. Similarly the 128-bit key is also depicted into a square matrix. The 128-bit key is expressed into an array of key schedule words: each word is of four bytes. The totals key schedule words for ten rounds are 44 words; each round key is similar to one state. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms, high calculation and computation overhead.

Image Encryption Using Block Based Transformation Algorithm

Mohammad Ali Bani Younes and Aman Jantan [16] proposed this technique. In this paper, we introduce a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm.

Image encryption using combination of permutation

Mohammad Ali Bani Younes and Aman Jantan [15] proposed a technique in which image is divided in to fixed size blocks (4 X 4). Increasing the number of blocks resulted lower correlation and higher entropy. Then blocks are transformed into new location using various permutation techniques. The generated image is then fed to the RijnDael encryption algorithm. Rijndael algorithm has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. The results showed that the correlation between image elements was significantly decreased and higher entropy was achieved.

Image encryption using least square approximation techniques

Mahmood Al-khassaweneh and Selin Aviyente [14] has put forth a new image encryption technique based on the concept of Least Square Approximation (LSA). In this paper, the translation of the original image into the form of encrypted one by the randomly generating vectors. And on the other hand the original image has been decrypted by using the least square approximation concept on the encrypted image and also on the randomly generating vectors. As the result of this, there is a good range of efficiency in this algorithm and also promotes good enhancement in the security aspects.

Image encryption using advanced hill cipher algorithm

Bibhudendra Acharya and et al. [13] proposed a novel advanced Hill (AdvHill) encryption technique which uses an involutory key matrix. The scheme is a fast encryption scheme which overcomes problems of encrypting the images with homogeneous background. AdvHill algorithm can be used for grayscale and color images. In this technique involutory key matrix of fixed size is

constructed and then plain image is divided into same size blocks. The ith pixels of each block are brought together to form a temporary block. Hill cipher technique is applied onto the temporary block.. The resultant matrix is transposed and Hill cipher is again applied to this matrix. The final matrix obtained is placed in the *i*th block of the encrypted image. Original Hill Cipher can't encrypt the images properly if the image consists of large area covered with same color or gray level. But this algorithm works for any images with different gray scale as well as color images.

Image encryption using DCT and stream cipher

Lala Krikor et al. [12] proposed a technique that is based on encrypting of (Discrete Cosine Transform) DCT coefficients. The DCT is a mathematical transformation that takes a signal and transforms it from spatial domain into frequency domain. JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images. This method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients correlated to the higher frequencies of the image block are encrypted using Non-Linear Shift Back. NLFSR consists of two 8-bits Shift Registers, with certain feedback functions, and the output of these two registers and XORed to give the pseudorandom bit sequence.Encrypting only some selective DCT coefficients based on the fact that the image details are situated in the higher frequencies, while the human eye is most sensitive to lower frequencies than to higher frequencies.

Image encryption using SCAN patterns and carrier images

Panduranga H.T and Naveen Kumar S.K [11] propose a hybrid technique for image encryption which employs the concept of carrier image and SCAN patterns generated by SCAN methodology. The SCAN is a formal language-based two dimensional spatial accessing methodology which can represent and generate a large number of wide varieties of scanning paths. SCAN language uses four basic scan patterns. They are continuous raster C, continuous diagonal D, continuous orthogonal O, and spiral S. Here the carrier image is created with the help of alphanumeric keyword. Each alphanumeric key will be having a unique 8bit value generated by 4 out of 8-code. This newly generated carrier image is added with original image to obtain encrypted image. The scan methodology is applied to either original image or carrier image, after the addition of original image and carrier image to obtain highly distorted encrypted image. The resulting image is found to be more distorted in hybrid technique. By applying the reverse process we get the decrypted image.

Image encryption using godelization method

B.V.Rama Devi et al. [10] proposed a method in which the image which is to be transmitted is transformed into a sequence called Godel Number Sequence (GNS) using a new technique called Godelization. This is compressed using Alphabetic coding (AC) and encrypted by an encryption method. Godelization method, it is a process of converting any positive integer which is greater than 1 into a sequence called Godel Number Sequence (GNS). If any image is represented by intensity values (i1, i2, ……. ,in), then each of these intensity values can be converted into a Gödel Number Sequence GNS[2]. Then GNS (i1)$GNS(i2)$.....$GNS(in) is called the Gödel String of the image. Alphabetic Coding (AC) is a process of compressing a given string of numbers. With AC technique the length is reduced same as run length encoding. In the third step compressed string will be encrypted using a symmetric key cryptosystem or a public key cryptosystem. This method works efficiently for images and as well as for text, while for large images Godelization requires some processing time which is not a big concern with the available hardware support today.

Permutation based image encryption technique

Sesha Pallavi Indrakanti et al. [9] have proposed a method for encryption which has three phases. This technique makes use of all the 3 types of classifications like position permutation, value and visual transformation. The first phase is the image encryption where the image is divided into blocks and these blocks are permutated. Further permutation is applied based on a random number to make stronger the encryption. The second phase is the key generation phase, where the values used in the encryption process are used to build a key. The third phase is the identification process which involves the numbering of the shares that are generated from the secret image. These shares and the key are then transferred to the receiver. The encryption process gives out 4 shares. Each of these shares has to be numbered distinctly for the identification process. All the 4 shares of the image are numbered uniquely with the same series. These numbers are embedded into the share in the form of a watermark. The same number series is kept in the key. The receiver will compare the number sequence of the shares with that in the key to compute the right secret with the valid shares. This

method can be extended in trying to handle multiple images instead of single image.

Image encryption using block based transformation algorithm

Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta [8] have proposed an Image Encryption technique in which the original image is divided into number of blocks which are shuffled within the image to build a newly transformed image. The generated (or transformed) image is then fed to the blowfish encryption algorithm and thus generated one can be viewed as an arrangement of blocks. Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor.

Image Encryption using Block-Based on Shifted Algorithm

Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush [7] propose a new algorithm. The first part of the algorithm aims to build a shifted table using hash function within encryption phase and decryption phase to generate an encrypted (shifted) image and the original image. The second part of the algorithm uses the shifted table resulted from the first part of the algorithm to generate newly shifted image in which the rows and the columns of the original image are shifted and followed by encryption technique to increase the security of the image encryption. This implies a high similarity and a good quality of the retrieved image compared to the original image.

Image Encryption by using Hyper Image Encryption Algorithm

Hiral Rathod et. al proposed this method [29]. The Proposed Architecture for encryption and decryption of an image using suitable user defined key. This paper introduces a new permutation technique based on the combination of image permutation and a new developed encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". From the selected image having binary value blocks, which will be rearrange into a permuted image using a permutation process, and then the generated image will be encrypted using the "Hyper Image Encryption Algorithm (HIEA)" algorithm.

5. Discussion and Future Scope

Efficient encryption of images and text is very critical job. As per my survey Blowfish has better encryption scheme than other algorithms. Secondly, AES has advantage over the other 3DES and DES in terms of throughput & decryption time except Blowfish. Third point is that 3DES has the least performance among all the algorithms mentioned here. In future the work can be extended by including various schemes and techniques over different types of data such as image, sound and video and developing a stronger encryption algorithm with high speed and least energy utilization.

6. References

[1] S.Pavithra, Mrs. E. Ramadevi " STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS " International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 5, July 2012 14 pp.82-86

[2] Shanta, yoti Vashishtha on " Evaluating the performance of Symmetric Key Algorithms:AES(Advanced Encryption Standard) and DES(Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ,pp.43-49

[3] Monika Agrawal,Pradeep Mishra "A Comparative Survey on Symmetric Key Encryption Techniques"International Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012, pp.877-882.

[4] Jawahar Thakur , Nagesh Kumar " DES , AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1,Issue 2,December 2011),pp.6-12

[5] Himani Agrawal and Monisha Sharma "Implementation and analysis various symmetric cryptosystems " in indian Journal of Science and Technology in Vol. 3 No.12 (Dec 2010) ISSN: 0974- 6846.pp.1173-1176

[6] Aamer Nadeem and Dr M. Younus Javed , "A Performance Comparison of Data Encryption Algorithms", IEEE, 2005.

[7] Ahmed Bashir Abugharsa, Abd Samad Bin HasanBasari and Hamida Almangush "A New Image Encryption Approach using Block-Based on Shifted Algorithm", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.12, December 2011.

[8] Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta "A New Image Encryption Approach Using

Block Based Transformation Algorithm ", (IJAEST) international journal of advanced engineering sciences and technologies Vol No. 8, Issue No. 1, 090 – 096, 2011.

[9]Sesha Pallavi Indrakanti and P.S.Avadhani "Permutation based Image Encryption Technique", International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, August 2011.

[10] B.V.Rama Devi, D.Lalitha Bhaskari, P.Prapoorna Roja, P.S.Avadhani "A New Encryption Method for Secure Transmission of Images", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2801-2804.

[11] Panduranga H.T and Naveen Kumar S.K, "Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images ", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 297-300.

[12] Lala Krikor, Sami Babaet., Thawar Arif, and Zyad Shaaban "Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research Vol.32 No.1 (2009), pp.47-57 ISSN 1450-216X

[13] 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.

[14]Mahmood Al-khassaweneh, Selin Aviyente,"Image Encryption Scheme Based on Using Least Square Approximation Techniques" IEEE Transactions, pp.108-111, 2008.

[15] Mohammad Ali Bani Younes and Aman Jantan, "An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, vol 3 no 4, April 2008.

[16] Mohammad Ali Bani Younes and Aman Jantan, "Image Encryption Using Block – Based Transformation Algorithm" IAENG, 35:1, IJCS_35_1_03, February 2008.

[17] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki "A Modified AES Based Algorithm for Image Encryption", World Academy of Science, Engineering and Technology 27 2007.

[18] Ameritech Mobile Communications et al., Cellular Digitalfacket Data Sjfstem Specifications: *Part 406:* Airlink Security, CDPD Industry Input Coordinator, Costa Mesa, Calif., July 1993.

[19] Accredited Standards Committee X9, Working *Draft:* American National Standard X9.30- *1* 993: Public Key Cryptography Using lrreversible Algorithms for the Financial Services Industry: *Part 4:* Management of Symmetric Algorithm Keys Using Diffie-Hellman, Am. Bankers Assoc., June 4, 1993.

[20] FlPS Publication *180: SecureHashStandard(SHS),* NIST, May 11, 1993.

[21] E. Bihamand A. Shamir, "Differential Cryptanalysisof theFulll6- Round DES," *Proc.* Crypto 92, Advancesin Cryptology, Springer-Verlag, New York, 1993, to appear.

[22] R.L. Rivest, The RC4 Encryption Algorithm, RSA Data Security, Inc., Mar. 12, 1992.

[23] NIST, "The Digital Signature Standard, Proposal and Discussion," *Comm.* ACM, Vol. 35, No. 7, July 1992, pp. 36-54.

[24] PKCS #3: Diffie-Hellman Key Agreement Standard, Version *I* .3, RSA Data Security, Inc., June 1991.

[25] FlPSPublication46-*1 :DataEncryptionStandard*N. IST, Washington, D.C., Jan. 22, 1988; originally issued by the National Bureau of Standards.

[26] Australian Standard 2805.5 1985: Electronics Funds Transfer- Requirements for Interfaces: *Part* 5-Data Encryption Algorithm, Standards Assoc. of Australia, North Sydney, NSW, 1985.

[27] Accredited Standards CommitteeX3,ANSlX3.92: Data Encryption Algorithm (DEA), ANSI, New York, 1981.

[28] W. Diffie and M.E. Hellman, "New Directions in Cryptography," */€€E* Trans. information Theory, Vol. IT-22, 1976, pp. 644-654.

[29] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, "Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3