Data Security by Video Steganography and Cryptography Techniques

Nishi Khan[1], Kanchan S. Gorde[2]
M.E. Student[1], Professor[2]
Terna Engineering College[1, 2]
nishikhan90@gmail.com [1], gordekanchan@yahoo.co.in[2]

Abstract: Cryptography and steganography are the two popular methods available to provide security. Cryptography and Steganography are well recognized and widely used methods that manipulate information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

In this paper we have proposed an advanced approach for vigorous data protection in which we have used key frame extraction technique, the cover-video is divided into RGB frames and using statistical features such as standard deviation, skewness and kurtosis, key frames has been extracted and the text message in binary form is embedded into key frames of stego video using LSB technique and hybrid approach in such a way that the video does not lose its functionality. Text message is encrypted using AES algorithm. As key frame extraction technique is completely new in video steganography so it becomes impossible for interloper to estimate that a text message is hidden in the video. The proposed system is simple and new and therefore can be used to transfer highly confidential data like military secrets, hospital reports and other data. This proposed method strives for high security to an eavesdropper's inability to detect hidden information.

Keywords: Security, Cryptography, Video Steganography, LSB, AES

I. INTRODUCTION

Cryptography systems can be roughly classified into symmetric-key systems that use a single key that both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message for instance, might produce suspicion on the part of the recipient while an invisible message created with steganographic methods will not. In fact, steganography can be useful when the use of cryptography is forbidden: where cryptography and strong encryption are outlawed, steganography can circumvent such policies to pass message covertly. However, steganography and cryptography differ in the way they are evaluated: steganography fails when the "enemy" is able to access the content of the cipher message, while cryptography fails when the "enemy" detects that there is a secret message present in the steganographic medium.
The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called cryptanalysis and steganalysis. The former denotes the set of methods for obtaining the meaning of encrypted information, while the latter is the art of discovering covert messages. The aim of this paper is to describe a method for integrating together cryptography and steganography through some media such as image, audio, video, etc.

II. CRYPTOGRAPHY

Cryptography is an essential section of any approach to address message communication security requirements. Cryptography is the study of methods of sending messages in concealed form so that only the intended recipients can remove the mask and read the message. It is the actual art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'. The message may be transformed using a 'code' (in which case each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual characters).Cryptology is the science underlying cryptography. Cryptanalysis is the science of 'breaking' or 'cracking' encryption schemes, i.e. discovering the decryption key. Cryptographic systems are broadly classified along three independent dimensions.

- **Methodology for transforming plain text to cipher text**

All encryption algorithms are mainly based on two general principles: substitution, in which each element in the plain text is mapped into another element, and substitution, in which elements in the plain text are rearranged. The fundamental condition is that no data should be lost.

- **Methodology for number of keys used**

There are some standards methods which are used with cryptography such as secret key, public key, digital signature and hash function.
Secret Key (Symmetric): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the

cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called as symmetric encryption.

Public Key: Public key cryptography has been said to be the most significant new growth in cryptography in the last 300-400 years. Modern Public Key Cryptography was first defined publicly by Standford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their study described a two-key crypto system in which two parties could engage in a secure communication over an insecure communications channel without having to share a secret key.

Digital Signature: The use of digital signature came from the need of endorsing the authentication. The digital signature is more like stamp or signature of the sender which is embedded together with the data and encrypts it with the private key in order to send it to the other party. In addition, the signature declares that any change made to the data that has been signed is easy to detect by the receiver.

Hash Function: The hash function is a one way encryption, the hash function is a well-defined method or mathematical formula that represents a small size of bits which is generated from a large sized file, the result of this function can be called hash code or hashes. The generating of hash code is faster than other methods which make it more desired for authentication and integrity. Cryptographic hash functions are much used for digital signature and cheap constructions are highly desirable. The usage of cryptographic hash functions for message authentication has become a standard approach in many applications, particularly internet security protocols. The authentication and the integrity considered as main issues in information security, the hash code can be attached to the original file then at any time the users are able to check the authentication and integrity after sending the secure data by applying the hash function to the message again and compare the result to the sender hash code, if it's similar that is mean the message came from the original sender without altering because if there is any changed has been made to the data will changed the hash code at the receiver side.

- **Methodology for processing plain text**

A block cipher processes the input one block of elements at a time, generating an output block for each input block. A stream cipher processes the input elements constantly, producing output one element at a time, as it goes along. The proposed algorithm uses a substitution cipher method. It is a symmetric key algorithm using the technique of stream cipher.

III. STEGANOGRAPHY

The word steganography comes from the Greek Steganos, which mean covered or secret and graphy means writing or drawing. Therefore, steganography means, literally, covered writing. The main goal or steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [4]. During the process, characteristics of these methods are to change in the structure and features so as not to be identifiable by human eye. Digital images, videos, sound files, and other computer files that contain perceptually unrelated or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover-image, a so-called stego image is obtained. The basic model of steganography consists of Carrier, Message, Embedding algorithm and Stego key. The model for steganography is shown in Figure 1. Carrier is also known as a cover-object, which embeds the message and assists to hide its presence.

Capacity, security and robustness are three different aspects affecting steganography and its usefulness. Capacity refers to the amount of information that can be hidden in the cover medium. Security relates to an eavesdropper's inability to detect hidden information and robustness is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.

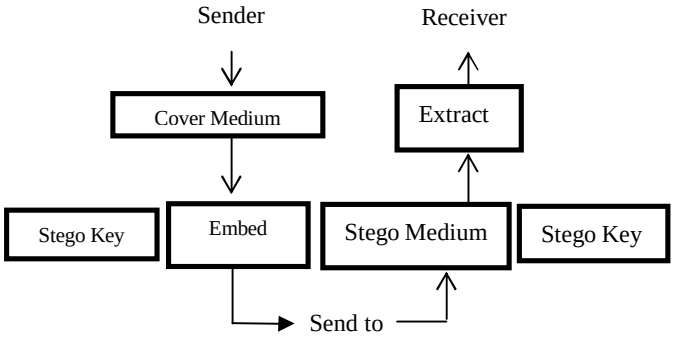

Fig 1: Block diagram of Steganography mechanism

IV. STEGANOGRAPHY IN DIGITAL MEDIUMS

To obtain security, there are different steganographic techniques depending on the type of the cover object.

- Image Steganography
- Network Steganography
- Video Steganography
- Audio Steganography
- Text Steganography
- Steganography using puzzles

V. STEGANOGRAPHY IN VIDEOS

Videos may use discrete frames that flash by too rapidly to be observed, but contain secret information when viewed as still images. Video images could also be altered in essentially the same ways as still images, and since video files are larger than single image files, more data could be hidden. Audio recordings may contain background "noise" that actually contains a message, or could be altered in a way that, like the modification of images discussed above, leaves the sound

natural, but reveals a message when compared against the original audio file.

VI. STEGANOGRAPHY VS CRYPTOGRAPHY

Basically, the purpose of cryptography and steganography is to provide secret communication. According to dictionary.com: Steganography is:" Hiding a secret message within a larger one in such a way that others cannot discriminate the presence or contents of the hidden message" and Cryptography is "The process or skill of communicating in, or deciphering secret writing or ciphers." Steganography can be used to cloak hidden messages in image, audio and even text files. It has until recently been the poor cousin of cryptography. Now, it is gaining new popularity with the current industry demands for digital watermarking and fingerprinting of audio and video. Steganography must not be confused with cryptography, where we transform the message so as to make its meaning ambiguous to malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated. The distinction between cryptography and steganography is an important one, and is summarized by the following table.

Table 1: Comparison of Steganography and Cryptography

Techniques	Steganography	Cryptography
Definition	Steganography means cover writing	Cryptography means secret writing
Objective	Focuses on keeping existence of a message secret	Focuses on keeping contents of a message secret
Key	Optional	Necessary
Carrier	Any digital media	Usually text based
Visibility	Never	Always
Security Services Offered	Confidentiality, authentication	Confidentiality, availability, data integrity, non-repudiation
Attacks	It is broken when attacker detects that steganography has been used known as Steganalysis	It is broken when attacker can read the secret message known as Cryptanalysis
Result	Stego file	Cipher text

VII. COMBINED CRYPTO-STEGANOGRAPHY

Steganography is not the same as cryptography. Data hiding techniques have been widely used to transmission of hiding secret message for long time. Ensuring data security is a big challenge for computer users. Business men, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel.

A pictorial representation of the combined concept of cryptography and steganography is depicted in figure 2.

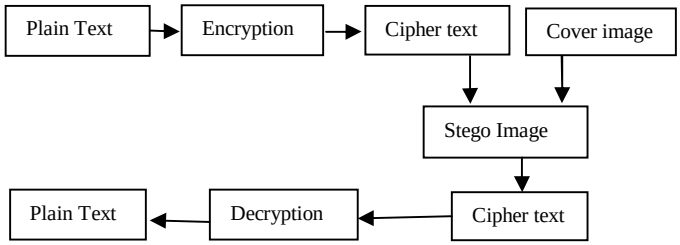

Fig.2. Combination of Steganography and Cryptography

In figure 2, both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Since then, the steganography approaches can be divided into three types:

Pure Steganography: This technique simply uses the steganography approach only without combining other methods. It is working on hiding information within cover carrier.

Secret Key steganography: The secret key steganography use the combination of the secret key cryptography technique and the steganography approach. The idea of this type is to

encrypt the secret message or data by secret key approach and to hide the encrypted data within cover carrier.

Public Key Steganography: The last type of steganography is to combine the public key cryptography approach and the steganography approach. The idea of this type is to encrypt the secret data using the public key approach and then hide the encrypted data within cover carrier.

VIII. LITERATURE SURVEY

In [1], authors discover the steganography, its history, features, tools and various techniques like LSB, masking, filtering and other transformations used for hiding messages in an image.

In [2], simple cryptographic concepts and techniques are defined. Various methods to hide the secret or confidential message in an original file is shown in this paper.

In [3], authors introduced the idea of embedding the secret message into an image using LSB technique and then applied AES algorithm to provide enhanced security.

In [4], author proposes a reverse procedure described in paper [3] by using an alteration component method.

In [5] user enters username, password and a key. A key is taken from automatic key generator device which generates a unique key after some specific time. After this the secret message and key is encrypted and encrypted message is embedded into cover image and stego image is produced.

In paper [6] the secret message is first compressed then the message is hashed and encrypted using encryption key. This method results in robust model and achieves two important principles of security i.e. privacy and authenticity.

In [7], authors proposed various technologies used in image steganography. This paper presents a review used for hiding a secret message or image in spatial and transform domain. This paper also proposed techniques for detecting the secret message or image i.e. steganalysis.

In [8] Author uses video file as a cover medium for steganography. Video based steganography can be used as one video file having separate images in frames. Since that the use of the video based steganography can be more eligible than other multimedia files therefore author is mainly anxious with how to embed data in a video file from bmp images and how we can make use of the inner structure of the video to hide data to be secured

In [9], A. Joseph Raphael introduces basic terminologies of cryptography and steganography and ensures that the combination of both gives multiple layers of security and will achieve requirements like capacity, security and robustness.

In [10] Based on similar concept with stenography it is desired to maximize the amount of hidden information while preserving security against detection by unauthorized parties. The image based stenography issues has been demonstrated to hide secret information in images and the possibility of using the image as a cover carrier for hiding secure data.

In [11] an image encryption algorithm merging the image encryption based on S-boxes scrambling with error correcting code was developed. The error correcting code could successfully improve the security of image encryption algorithm based on S-boxes scrambling. The basic concept of this author is on maximizing security, capacity factor of data hiding and secures the data through AES.

The authors in paper [12] introduced the method for embedding the secret image into cover image using LSB technique and then encrypts using DES algorithm and used the key image.

In [13] the author has proposed an AES technique which grants fundamental mathematics behind the algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security. AES provides better security and has less implementation complexity. It has been developed as one of the strongest and the most efficient algorithm.

In [14], authors first encrypts the data with RC4 encryption algorithm and then embeds in BMP cover image using three different steganographic methods and then compares these three methods. This paper also results in achieving the requirements of security i.e. data confidentiality, data integrity and data authentication.

The paper at [15], embeds the secret image into 24 bit or 8 bit image by using LSB and then evaluated results for 2, 4, 6 LSB for a .png file and a .bmp file.

In [16], authors proposed a new technique called metamorphic cryptography where secret image is encrypted and transformed into a cipher image using key and this cipher image is embedded into a cover image by converting it into an intermediate text and finally transformed once again into an image.

In the paper at [17], authors define basic terminologies of steganography, steganography techniques, classifications and review of previous work done by researchers.

In [18] author uses an algorithm based on AES expansion in which the encryption process is a bit wise exclusive or operation of a set of image pixels along with the 128 bit key, which differ for every set of pixel. The keys to be used are generated independently at the sender and receiver side based on AES key expansion process. Hence the initial key is shared rather than scaring the whole set of keys. The author gives the information about AES. The AES delivers high encryption quality with minimum memory requirement and computational time.

In [19] author gave a different concept from above the authors using a new approach of hiding image in video. The algorithm replaces 1 LSB of each pixel in video frame. It becomes very difficult for an intruder to guess that an image is hidden in the video as individual frame are difficult to analyze in a video running at 30 frames per second. We have seen that the author has used only 1 LSB substitution technique here.

In [20], the secret message or data can be hidden in any image, audio or video which provides more security. The secret data is first encrypted using AES algorithm and key is hashed using SHA-1 to prevent from attacks then user can hide the cipher data in image, audio or video using LSB technique. The receiver should provide the same key that is hashed for encryption.

In [21], the method is similar to that in the paper [6]; the only difference is the compressed message is not hashed. This

novel approach requires less memory space, fast transmission rate, better security and no distortion in quality of image.

In the paper at [22], authors proposed two methods to ensure high security. First method includes the combination of both steganography technique and cryptography technique and second method only includes steganography approach.

IX. THE PROPOSED MECHANISM

- PROPOSED ALGORITHM

1) *Embedding Algorithm:*

- Input Video.
- Extract the frames of the given video.
- Using statistical features extract the key frames (K).
- Insert secret data in K-1 frame.
- The LSB position of each K-1 frame will be used to store the secret data.
- Store key frame index number in the LSB of the last frame of the video.
- Combine all the K-1 frames and key frames to generate the video sequence this is the Stego video i.e. encrypted video.

*secret data is the data from text file in binary format.

2) *Extracting Algorithm:*

- Input the Stego video.
- Extract the frames from the Stego video.
- Get the last frame and read the LSB to get the key frame index.
- Extract the K-1 frames based on the index of the key frame.
- Read the secret data from LSB of each K-1 frame.
- Combine the data read from each K-1 frame to get the secret message.

X. METHODOLOGY

A. Algorithm of shot boundary detection

Many approaches used different kinds of features to detect shot boundary, including histogram, shape information, motion activity. Among these approaches, histogram is the popular approach. However, in these histogram-based approaches, pixels' space distribution was neglected. Different frames may have the same histogram. divided each frame into r blocks, and the difference of the corresponding blocks of consecutive frames was computed by color histogram. The color histogram contains only the frequency of a color value, but loses the pace information of the pixels. Therefore, in order to get the spatial distribution information of the color, the image is usually divided into appropriate blocks. If the blocks of the image are too small, it cannot be partitioned. More image blocks can improve the spatial resolution of the image, but it also increases the storage space of the image characteristics.

Algorithm steps are as follows.

Step 1: Partition the frame into m*n blocks .B(i,j,k) stands for the block of i,j at the kth frame.

Step 2: Computing x2 histogram matching difference between all blocks of single frame.

Step 3: Compute mean (MD), standard variance (STD), skewness (S) and kurtosis (k) for a single frame.

Step 4: Compute difference of these four values from two consecutive frames

MD=MDi-MD(i+1)

STD=STDi-STD(i+1)

S=Si-S(i+1)

K=Ki-K (i+1)

Where i and i+1 are two consecutive frames.

Step 5: Add all four differences to and out total difference Td

Td=MD+STD+S+K Step 6: Calculate threshold

T = Md + _STD

Step 7: Compare Td with threshold.

Step 8: If Td(i; i+1) _ T then i is the end of previous shot and i+1 is start of next shot.

B. Key Frame Extraction

A key frame is a frame that best represents the video content in an abstract manner. In proposed system to extract key frames above algorithm of shot boundary detection is applied over video sequence .Then from every shot a frame with highest mean and standard deviance is extracted. So, from every shot one key frame is extracted to form static video summarization.

Algorithm of key frame extraction

Step 1: Divide the whole video sequence into shots using above algorithm.

Step 2: Find frame with maximum mean and standard variance from each shot.

Step 3: These frames form static summarization.

C. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm and U.S. government standard for secure and classified data encryption and decryption.

In December 2001, the National Institute of Standards (NIST) approved the AES as Federal Information Processing Standards Publication (FIPS PUB) 197, which specifies application of the Rijndael algorithm to all sensitive classified data.

The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN) and does not use the Data Encryption Standard (DES) Feistel network.

The AES replaced the DES with new and updated features:

- Block encryption implementation

- 128-bit group encryption with 128, 192 and 256-bit key lengths
- Symmetric algorithm requiring only one encryption and decryption key
- Data security for 20-30 years
- Worldwide access
- No royalties
- Easy overall implementation

XI. CONCLUSION

In this paper a very comprehensive review of both steganography and cryptography techniques has been discu ssed for the security of transmitted data over the data networks but lacks in some way or the other as far as their individual abilities related to exposure of all the security principles are concerned. So, in order to overcome the lack of coverage of all the principles of security in those algorithms, a new algorithm has been proposed that would satisfy all the principles of security and also satisfy the requirements of steganography.

The proposed algorithm can be implemented in a security system as a future research work that would probably surpass in comparison to the existing algorithms. The system would be tested on the basis of various test cases such as MSE and PSNR and the results would be compared with those of existing algorithms.

REFERENCES

[1] Neil F. Johnson, Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, Feb1998, pp. 26-34.

[2] F. Piper, "Basic Principles of Cryptography", IEEE Colloquium on Public uses of Cryptography, April 1996, pp. 2/1-2/3.

[3] Dr. R. Sridevi, Vijaya Lakshmi Paruchuri, K.S. Sadasiva Rao, "Image Steganography combined with Cryptography", International Journal of Computers & Technology, ISSN: 22773061, Vol.9, July 2013, pp. 976-984.

[4] Lokesh Kumar, "Novel Security Scheme for Image Steganography using Cryptography Technique", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X Vol.2, April 2012, pp. 143-146.

[5] Mihir H Rajyaguru, "Crystography -Combination of Cryptography and Steganography with Rapidly Changing Keys", International Journal of Emerging Technology and Advanced Engineering, ISSN: 2250-2459, Vol.2, October 2012, pp. 329-332.

[6] H.Al-Barhmtoshy, E.Osman and M.Ezzaand, "A Novel Security Model Combining Cryptography and Steganography", Technical Report, 2004, pp. 483-490.

[7] S.Ashwin, J.Ramesh, K.Gunavathi, "Novel and Secure Encoding and Hiding Techniques Using Image Steganography: A Survey", IEEE Xplore International Conference on Emerging Trends in Electrical Engineering and Energy Management, Dec 2012, pp. 171-177.

[8] A.K. Al Frajat, "Hiding data in video file An overview" Journal of applied sciences 10(15):1644-1649, 2010.

[9] A. Joseph Raphael, Dr. V.Sundaram, "Cryptography and Steganography-A Survey, International Journal of Computer and Technology Applications", ISSN: 2229-6093, Vol.2 (3), 2010, pp. 626-630.

[10] Ali K Hmood, "An overview on hiding information technique in images" Journal of applied sciences 10(18)2094-2100, 2010.

[11] Niu Jiping, "Image encryption algorithm based on rijndael S-boxes" in IEEE applied International conference on computational intelligence and security 978-0-7695-3508-1\08, 2008.

[12] R.Nivedhitha, Dr.T.Meyyappan, "Image Security using Steganography and Cryptographic Techniques", International Journal of Engineering Trends and Technology, ISSN: 2231-5381, Vol.7, 2012, pp. 366-371.

[13] Punita Meelu ,"AES Asymmetric key cryptographic system" in international journal of information technology and knowledge management, volume 4, 113-117, 2011.

[14] Wai Wai Zin, "Implementation and Analysis of Three Steganographic Approaches", IEEE Xplore International Conference on Computer Research and Development, March 2011, pp. 456-460.

[15] D. Jacobs, Snehal Kamalapur, Neeta Sonawane, "Implementation of LSB Steganography and its Evaluation for Various Bits", IEEE Xplore International Conference on Digital Information Management, Dec 2006, pp. 173-178.

[16] N.V Rao, J.TL Philjon, "Metamorphic Crypto- A Paradox between Cryptography and Steganography using Dynamic Encryption", IEEE Xplore International Conference on Recent Trends in Information Technology, June 2011, pp. 217-222.

[17] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Technique", International Journal of Advanced Science and Technology, Vol. 54, 2013, pp. 113-124.

[18] B. Subramanan, "Image encryption based on AES key expansion" in IEEE applied second international conference on emerging application of information technology, 978-0-7695-4329-1/11, 2011.

[19] Saurabh Singh, "Hiding Image to Video" International Journal of engineering science & technology Vol. 2(12), 6999-7003 ,2010

[20] Shery Elizabeth Thomas, Sumod Tom Philip, Sumaya Nazar, Ashams Mathew, Niya Joseph, "Advanced Cryptographic Steganography using Multimedia Files", International Conference on Electrical Engineering and Computer Science (ICEECS), May 2012, pp. 239-242.

[21] M. Sitaram Prasad, S. Nagan Janeyulu, Ch. Gopi Krishna, C. Nagaraju, "A Novel Information HidingTechnique for Security by using Image Steganography", Journal of Theoretical and Applied Information Technology, 2005-2009, pp. 35-39.

[22] Khalil Challita, Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and their Applications (IJNCAA), ISSN: 2220-9085, Vol. 1(1), 2011.

Authors:

Nishi Khan received her B.E. degree in the field of Electronics Engineering from RTMNU University in 2013 and pursuing M.E. in the field of Electronics Engineering from Terna Engineering College, Navi Mumbai, India. Her research interests include

image processing, steganography and cryptography. She has represented research paper in International conference as well as journal.

Kanchan S. Gorde is currently working as an Assistant Professor in Department of Electronics Engineering in Terna Engineering College, Navi Mumbai, India. She has more than 10 years of experience in teaching. She has represented various papers in International journals and in international as well as national conferences.