http://dx.doi.org/10.21172/ijiet.82.035

An Efficient Data Hiding Approach on Digital Colour Image for Secret Communication

Dr.K.S.Thivya,
Assistant professor
Department of Electronics and Communication Engineering
Easwari Engineering College,Chennai,TamilNadu,India

K.Suriyakrishnaan
Assistant professor
Department of Electronics and Communication Engineering
Easwari Engineering College,Chennai,TamilNadu,India

S.Sindhuja
Department of Electronics and Communication Engineering
Easwari Engineering College,Chennai,TamilNadu,India

Yamuna
Department of Electronics and Communication Engineering
Easwari Engineering College,Chennai,TamilNadu,India

Abstract- Reversible data hiding in encrypted images provides an excellent privacy security and protection. The success of the previous methods in this area has proved that by exploiting the redundancy within the image a superior performance can be achieved. Specifically, because the pixels in the local structures have a strong similarity, they can be heavily compressed, thus resulting in a large hiding room. In this paper, to better explore the correlation between neighbour pixels, we propose to consider the triple data encryption standard when hiding the secret data. The dictionary method is used to obtain the image lossless and to maintain the image quality. The widely used sparse coding technique has demonstrated that a patch can be linearly represented by some atoms in an over complete dictionary. As the sparse coding is an approximation solution, the leading residual errors are encoded and self-embedded within the cover image.

Keyword–Cryptography, Hashing, PSNR, TDES.

I. INTRODUCTION

Signal processing deals with the processing or transferring of ion contained in many different physical, symbolic, or abstract formats broadly designated as signals. Digital signal processing (DSP) uses computers to perform a wide variety of signal processing operations. The signals processed in this manner are nothing but a sequence of numbers. These numbers represent the samples of a continuous variable in a domain such as time, space, or frequency. It uses mathematical, statistical, computational, heuristic, and linguistic representations, formalisms, and techniques for representation, modelling, analysis, synthesis, discovery, recovery, sensing, acquisition, extraction, learning, security, or forensics.

Instead of trying to keep the PSNR value high, the proposed algorithm enhances the contrast of a host image to improve its visual quality. The highest two bins in the histogram are selected for data embedding so that histogram equalization can be performed by repeating the process.[1]"Analog" indicates something that is mathematically represented as a set of continuous values. This differs from "digital" which uses a series of discrete quantities to represent signal. The voltage, electric current or electric charge around components in the electronic devices is typically represented as analog values. An error or noise affecting such physical quantities will result in a corresponding error in the signals represented by such physical quantities [2].

Convolution is the basic concept in signal processing that states an input signal can be combined with the system's function to find the output signal. It is the integral of the product of two waveforms after one has reversed and shifted. Reversible data hiding is the work was in getting familiarised as the results are promising. Reversible data-hidings insert information bits by modifying the host signal, but enable the exact (lossless) restoration of the original host signal after extracting the embedded information. Expressions like distortion-free, invertible, lossless or erasable watermarking are sometimes used as synonyms for reversible watermarking [3].

1.1 Types of Encryption

It is a process of coding information .It could either be a file or mail message into cipher text. It is a form of unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. A key in cryptography is a long sequence of bits used by encryption / decryption algorithms. The following example to represents a hypothetical 40-bit key: 10101001 10011110 00011100 01010101. Depending on the type of encryption, information can be displayed as various numbers, letters, or symbols. Those who work in cryptography fields make it their job, to encrypt information or to break codes to receive encrypted information.

Manual encryption is a type which makes use of encryption software. These are computer programs that encrypt various bits of information digitally. The files wants to encrypt are chosen, and then an encryption type is chosen from a list that the security system provides. Transparent encryption is another type of computer software encryption. It can be downloaded onto a computer to encrypt everything automatically. One of the most important secure types of encryption available because it doesn't leave anything that might be forgotten when using manual encryption. In case a computer is stolen, if the executable applications and files has an encrypted copy then that can withstand power surges and protects information.

1.2 Symmetric Encryption

All encryption is done via a computer software program. We can easily encrypt information by ourselves. Symmetric encryption is one of the simplest ways for doing this . Here, a letter or number coincides with another letter or number in the encryption code. We can take any written text and substitute letters and numbers for their coded counterpart, thus encrypting the text.

1.3 Asymmetric Encryption

Asymmetric encryption is a secure and easy way that can be used to encrypt data that you will be receiving. It is generally done electronically. A public key is generated and is given to whomever you want or posted for the public to see. They can encrypt information using the key and send it to you. This is often done when writing emails. The data can be encrypted by the public key , the person who has the private key only can read the data again.

1.4 Types of Decryption

In symmetric decryption, the same mathematical equation both encrypts and decrypts the data. The following example, a simple letter substitution cipher, such as A=B, B=C, etc., is symmetrical because you simply reverse the process to decrypt the message. If they send a message using a symmetric encryption method, the recipients must also have the key to decrypt the document**.** A system involving a pair of linked keys known as public-key decryption is used in Asymmetric decryption method. In this system, anything encoded with one key requires the other key to decrypt, and so on. When they encode a message using someone’s public key, they know that only a recipient possessing the corresponding private key can read it.

1.5 Hashing

Hashing is a form of encryption that uses a specialized one-way encryption key. If they hash a given volume of data, it will produce a unique output string to that data, but it is impossible to reconstruct the data from the output string. They can re-encode the original data and compare it to the result string to verify it. This can serve as a type of error correction in encoding. Hashing a message and providing that value to their correspondents ensures that they can hash the message themselves and compare the values. As long as the two output strings match, recipients know the message is complete and unaltered.

II. PROPOSED ALGORITHM

2.1) Sparse Representation

The sparse representation of natural signals can be achieved by exploiting sparsity or compressibility. Natural signal is said to be sparse signal if that can be compactly expressed as a linear combination of a few small number of basis vectors. The key idea behind sparse signal processing field is that many real-world signals admit a parsimonious representation in some basis, which could be incorporated as a prior in solving many inverse problems in signal and image processing, including the very sampling mechanism by which the signal is acquired. Sparsity has played a key role in compression of signals such as speech, electrocardiogram signals, images, videos, etc. The recent thrust in the field has been to solve various inverse problems within the framework of sparsity. The sparsity constraint enables one to find unique solutions even in the case of under determined system of equations. The field has strong links to convex optimization, machine learning linear algebra, Bayesian estimation, dictionary learning, etc.

2.2) K-SVD Dictionary Learning

In recent years there has been a growing interest in the study of sparse representation of signals. Compression, regularization in inverse problems, feature extractions are some of the applications that use sparse representation . Recent activity in this field has concentrated mainly on the study of pursuit algorithms that decompose signals with respect to a given dictionary. To better fit the above model dictionaries can be designed by either adapting the dictionary to a set of training signals or selecting one from a pre-specified set of linear transforms. They propose a novel algorithm for adapting dictionaries in order to achieve sparse signal representations. They seek the dictionary that leads to the best representation for each member in this set, under strict sparsity constraints. They present a new method—the K-SVD algorithm—generalizing the K-mean Clustering process. Inorder to better fit the data K-SVD alternates between sparse coding of the examples based on the current dictionary and a process of updating the dictionary atoms. The update of the dictionary columns is combined with an update of the sparse representations, thereby accelerating convergence. Since K-SVD algorithm is flexible it can work with any pursuit method (e.g., basis pursuit, matching pursuit or FOCUSS). They analyse this algorithm and demonstrate its results both on synthetic tests and in applications on real image data.

2.3) Triple Data Encryption Standard

To each data block Data Encryption Standard (DES) cipher algorithm is applied three times by Triple Data Encryption Algorithm (Triple DEA or TDEA),which is a block cipher and a symmetric key. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute force attacks feasible. Without the need to design a completely new block cipher algorithm, Triple DES provides a simple way of increasing the key size of DES inorder to protect against such attacks.

2.4) Cryptography

The DES most widely used symmetric key cryptographic method is the Data Encryption Standard (DES). A fixed length, 56-bit key and an efficient algorithm to quickly encrypt and decrypt messages is used. It can be easily implemented in the encryption and decryption process even faster. One of the simplest way to make the system more secure is to increase the key size . A variation of DES, called Triple- DES or DES - EDE (Encrypt-Decrypt-Encrypt), uses three applications of DES and two independent DES keys to produce an effective key length of 168 bits. It has a fundamental weak spot-key, despite of the efficiency of symmetric key cryptography. In 1991 James Massey invented International Data Encryption Algorithm (IDEA). IDEA uses a fixed length, 128-bit key (larger than DES but smaller than Triple-DES). It is also faster than Triple- DES. The algorithms RC2 and RC4 was invented by Don Rivest of RSA Data Security. These use variable length keys and are claimed to be even faster than IDEA

III. TRIPLE DATA ENCRYPTION ALGORITHM

3TDES key K is first generated and distributed by the users before using TDES, which consists of three different DES keys K_1, K_2 and K_3. This means that the actual 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows

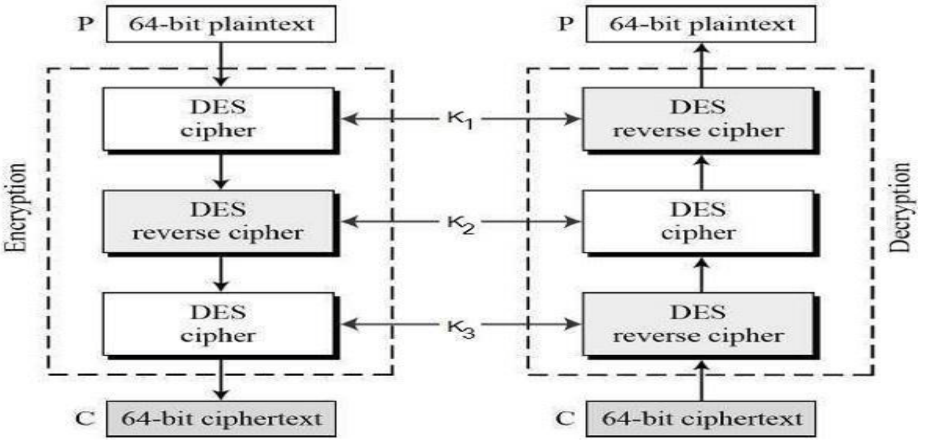


Figure 2.Block Diagram of Tripple Data Encryption

The encryption-decryption process is as follows 1)Encrypt the plaintext blocks using single DES with key K_1.
2) Now decrypt the output of step 1 using single DES with key K_2. 3).Finally, encrypt the output of step 2 using single DES with key K_3. The output of step 3 is the cipher text. Decryption of a ciphertext is a reverse process. K_3 is first used by the user to decrypt then K_2 is used to encrypt , and finally K_1 to decrypt . Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting $K_{1,}$ $K_{2,}$ and K_3 to be the same value.

This provides backwards compatibility with DES. Except that K_3 is replaced by K_1 , Second variant of Triple DES (2TDES) is identical to 3TDES. In other words, user encrypt plaintext blocks with key $K_{1,}$ then decrypt with key $K_{2,}$ and finally encrypt with K_1 again. Therefore, 2TDES has a key length of 112 bits. Triple DES systems are significantly more secure than single DES, but these are clearly a much slower process than encryption using single DES. There are three keying options in data encryption standards: 1) All keys being independent 2) key 1 and key 2 being independent keys 3) All three keys being identical. The triple DES key length contains 168 bits but the key security falls to 112 bits

3.1) Working of TDES

Run DES three times: ECB mode: If K2 = K3, this is DES Backwards compatibility Known not to be just DES with

K4 Has 112 bits of security, not 3, 56 = 168. Triple DES algorithm uses three iterations of common DES cipher. It receives a secret 168-bit key, which is divided into three 56-bit keys

- Encryption using the first secret key.
- Decryption using the second secret key.
- Encryption using the third secret key

3.1.1) Encryption

c = E3 (D2 (E1 (m))) (1)

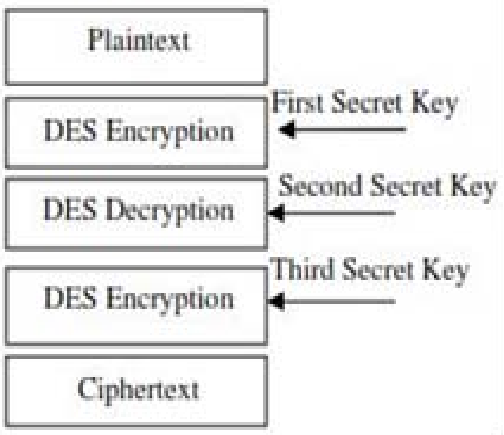


Figure 3 Block Diagram of Encryption

3.1.2) Decryption
m = D1 (E2 (D3(c))) (2)

Using decryption in the second step during encryption provides backward compatibility with common DES algorithm. In these case first and second secret keys or second and third secret keys are the same whichever key.

c = E3 (D1 (E1 (m))) = E3 (m) (3)

c = E3 (D3 (E1 (m))) = E1 (m) (4)

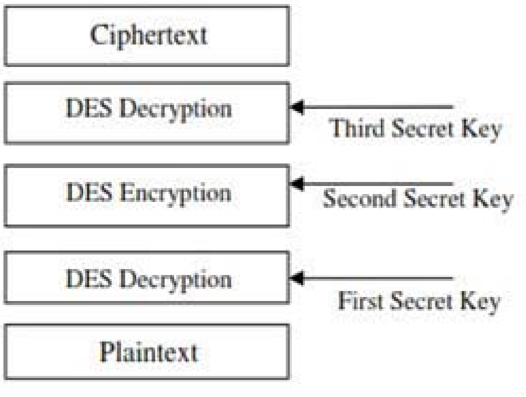


Figure 4 Block Diagram Of Decryption

It is possible to use 3DES cipher with a secret 112-bit key. In this case first and third secret keys are the same.

$$c = E1\ (D2\ (E1\ (m))) \qquad (5)$$

Compared to other encryption modes, Triple DES has a significantly sized key length. DES algorithm was replaced by the Advanced Encryption Standard and Triple DES is now considered to be obsolete. It is derived from single DES . This technique is used in triplicating and it involves three sub keys and key padding when necessary. Keys must be increased to 64 bits in length known for its compatibility and flexibility can easily be converted for Triple DES inclusion.

3.2) Encrypted Image Generation

For the image owner, to generate encrypted images, three phases: 1) Sparse representation 2) Self-reversible embedding 3) Stream encryption. Given a cover image, we first divide it into patches that are then represented according to an over complete dictionary via sparse coding. Then, the smoother patches with lower residual errors are selected for room reserving. These selected patches are represented by the sparse coefficients, and the corresponding residual errors are encoded and reversibly embedded into the other non-selected patches with a standard RDH algorithm. Finally, the room preserved and self-embedded image is encrypted to generate the final version.

3.3) Data Hiding In Encrypted Images

Once the encrypted image is received, the data hider can embed secret data for management or authentication requirement. The embedding process starts with locating the encrypted version of area A. Since the the position of the first room preserving patch and the room size for each patch image has been embedded by the owner in the encrypted image, it is effortless for the data hider to know where and how many bits they can modify. After that, the data hider scans each selected patch in the encrypted image and simply makes use of bit replacement to substitute the corresponding bits reserved for secret data. Here, we assume the selected patch number is denoted as C, our MER for the data hider is computed as follows,

$$\mathrm{MER} = \frac{C \times \left(8N^2 - L(n^p + n^v) - n^b\right) - n^a}{N_1 \times N_2} \qquad (6)$$

Where n^a is the dictionary size and is fixed for our algorithm. After data hiding, the position of the first data hiding patch and the hiding room size for each patch are also embedded into the encrypted image containing additional embedded.

3.3.1) Data Encryption Standard

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

3.4) Initial and Final Permutations

The initial and final permutations are straight Permutation boxes (P-boxes) that are inverses of each other. They have no cryptography significance in DES.

3.4.1) Voice Signal Encoding

After the image is encrypted using T-DES algorithm, the voice signal is taken as input which has to hidden in the image. The voice signal and the encrypted image is vectored and if the image size and the audio signal size varies then additional zeroes are added to make both the image and audio signal size equal. Then the binary datas of the image and the signal is merged alternatively, that is the first binary digit of the image and the first binary digit of the audio signal is arranged alternatively and so on. After the image and the signal is alternatively merged, the image will be hidden with the secret audio file which is given as input.

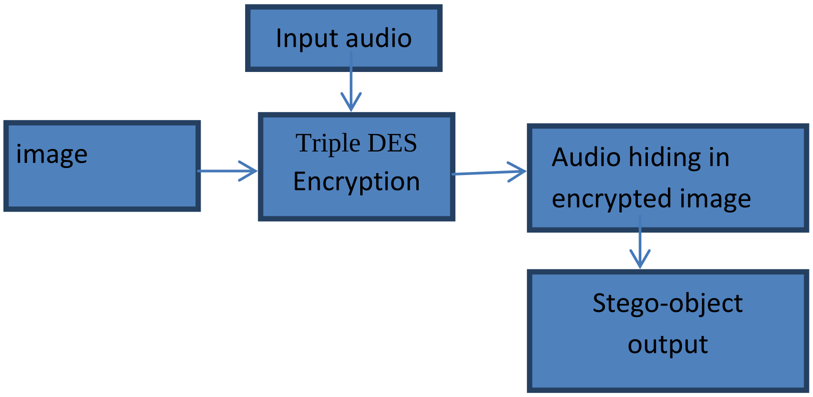


Figure 5.Block Diagram Of Voice Signal Encoding

3.4.2) Voice Signal Decoding

After the encoding is done the image is sent to the receiver, the receiver will decode the signal using the code given. The audio signal and the input image will get decoded by rearranging the binary data's which was alternatively merged while encoding and the additional zeroes given to the input will get removed and the original voice data and the image will be obtained lossless.

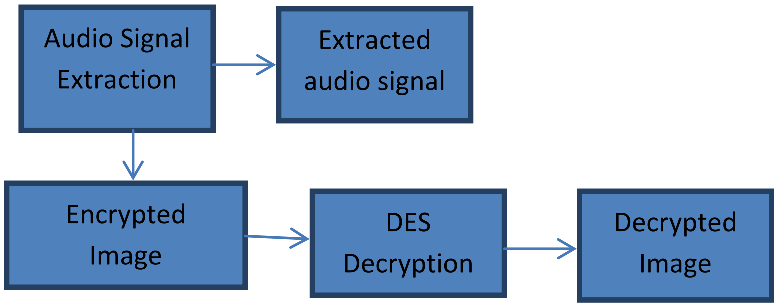
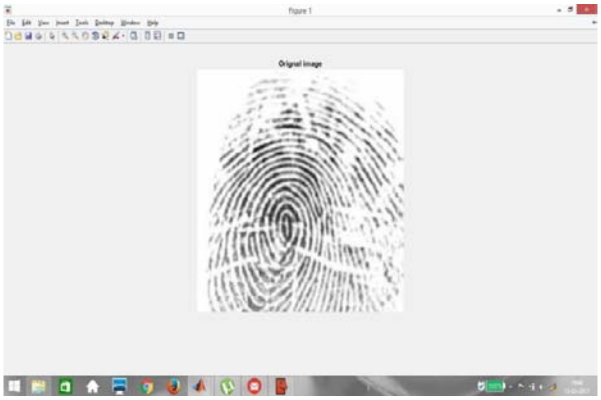
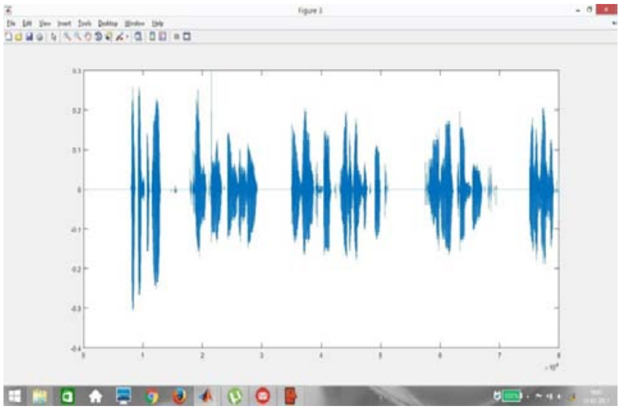


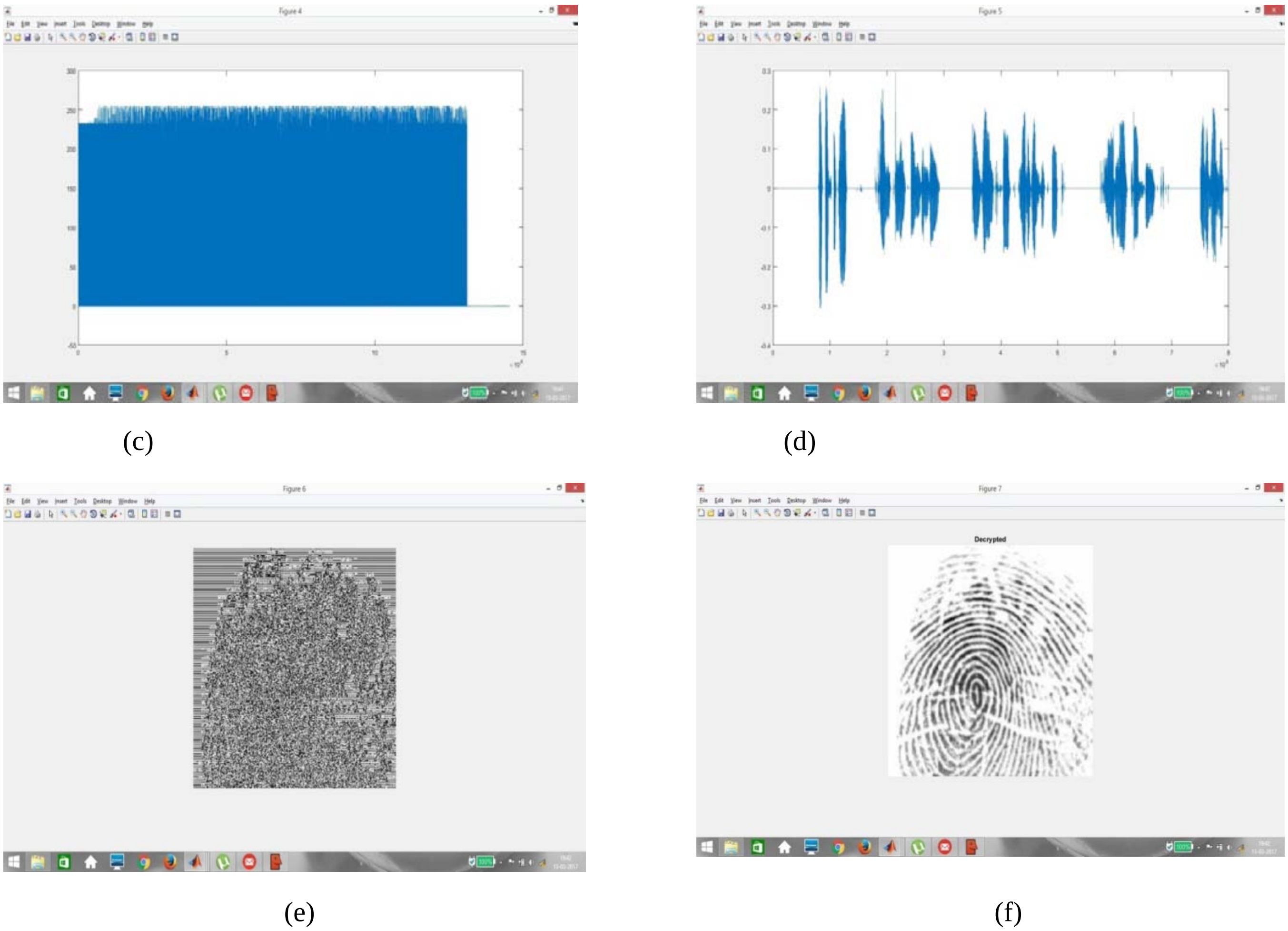
Figure 6.Audio Signal Extraction and Decryption

III. RESULTS AND DISCUSSION

To enhance the system for secret data communication over unsecure channel based on Colour Image and Encrypted data hiding using K-SVD Dictionary and Triple Data Encryption Standard (TDES).







(c)

(d)

(e)

(f)

Figure 4: Spectrum of a (a) Input Image (b) Encrypted Image (c) Input Audio (d) Encrypted Audio
(e) Decrypted Audio (f) Original Image

IV. CONCLUSION

The voice signal is efficiently hidden into the image using Triple data encryption standard and sparse representation. The results show that the audio signal and the output image obtained is lossless. The signal hiding method can be efficiently used in various fields for transferring secret message through an unsecured path. This method can be further developed in future by giving the input audio of our desired size and use more efficient data hiding algorithm which can hide 512 bits in a particular image.

REFERENCES

[1] Coltuc.D and J.-M. Chassery, “Very fast watermarking by reversible contrast mapping,” *IEEE Signal Process. Lett.*, vol. 14, no. 4, pp. 255–258, Apr. 2007.

[2] Fridrich,J , Goljan, M., Du, R., “Invertible Authentication”, Proc. SPIE,Security and Watermarking of Multimedia Contents, San Jose, California, 2001.

[3] Fridrich, J., Goljan, M., Du, R., “Reliable Detection of LSB Steganography in Grayscale and Color Images”,*Proc. ACM Special Session on Multimedia Securityand Watermarking*, Ottawa, Canada, 2001.

[4] Fridrich.J, M. Goljan and R. Du, "Invertible authentication watermark for JPEG images", *Proc. Inf. Technol. Coding Comput.*,pp. 223-227.

[5] Gao.M.Z , Z.-G.Wu, and L.Wang, "Comprehensive evaluation based contrast enhancement techniques," *Adv. Intell. Syst. Applicat* .,vol. 2, pp. 331–338, 2013.

[6] Goljan, M., Du, R., "Invertible Authentication Watermark for JPEG Files", *Proc. ITCC*, LasVegas, Nevada, April, 2001.

[7] Goljan M., Fridrich, J., and R. Du, "Distortion-free Data Embedding for Images", *The 4th Information Hiding Workshop*, Pittsburgh, Pennsylvania, April 25–27, 2001.

[8] Howard.P.G, F. Kossentini, B. Martins, S. Forchhammer, and W. J.Rucklidge,"The emerging JBIG2 standard," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 8, no. 7, pp. 838–848, Jul. 1998.

[9] Honsinger . C. W., "A Robust Data Hiding Technique Based on Convolution with a Randomized PhaseCarrier", *Proc. Of PICS'00*, Portland, Oregon, March, 2000.

[10] Hao-Tian Wu "Reversible Image Data Hiding with Contrast Enhancement"*IEEE SIGNAL PROCESSING*, vol. 22, NO. 1,JAN 2015.

[11] Jones. P., Rabbani, M., Stoffel, J. C., "Lossless Recovery of an Original Image Containing Embedded Data", US Patent application, Docket No:77102/E D, 1999.

[12] Li.X, B. Yang, and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524–3533, Jan. 2011.

[13] Long. M, Fridrich.J., "Steganalysis of LSB Encoding in Color Images", *Proc.ICME 2000*, NewYork City, New York, 2000.

[14] Macq, B., "Lossless Multiresolution Transform for Image Authenticating Watermarking", *Proc. Of EUSIPCO*, Tampere, Finland, September, 2000.

[15] Ni.Z, Y. Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," *IEEETrans. Circuits Syst. Video Technol.*, vol. 16, no. 3, pp. 354–362, Mar.2006.

[16] Sachnev.V , H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Trans.Circuits Syst. Video Technol.*, vol. 19, no. 7, pp. 989–999, Jul. 2009.

[17] Stark.J.A, "Adaptive image contrast enhancement using generalizations of histogram equalization," *IEEE Trans.Image Process.*, vol. 9,no. 5, pp. 889–896,May 2000.

[18] Sayood.K. : *Introduction to Data Compression*, Morgan Kaufmann Publishers, San Francisco, California, pp.87 94, 1996.

[19] Thodi.D.M and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Trans. Image Process.*, vol. 16, no. 3,pp. 721–730, Mar. 2007

[20] Wu.H.T and J. Huang, "Reversible image watermarking on predictionerror by efficient histogram modification," *Signal Process.*, vol. 92, no.12, pp. 3000–3009, Dec. 2012.

[21] Yang.Y, X. Sun, H. Yang, C.-T. Li, and R. Xiao, "A contrast- sensitive reversible visible image watermarking technique," *IEEE Trans. Circuits Syst.Video Technol.*, vol. 19, no. 5, pp. 656–667, May 2009.

[22] Zhao.Z, H.Luo,Z.-M. Lu, and J.-S. Pan, "Reversible data hiding basedon multilevel histogram modification and sequential recovery," *Int. J.Electron.Commun. (AEÜ)*, vol. 65, pp. 814–826, 2011.

[23] Zeng.T, X. Li, B. Ying , "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection", *IEEE Trans. Image Process.*, vol. 20, no. 12, pp. 3524-3533, Dec. 2011.