International Association of Scientific Innovation and Research (IASIR)
(An Association Unifying the Sciences, Engineering, and Applied Research)

ISSN (Print): 2279-0063
ISSN (Online): 2279-0071

International Journal of Software and Web Sciences (IJSWS)
www.iasir.net

Stegnography Using Interpolation and LSB With cryptography on Video Images

[1]Dr. Kulvinder Singh, [2]Dr. Sanjeev Dhawan, [3]Jagdeep Kaur
[1,2]Faculty of Computer Sc. & Engg, [3]M.Tech. Student,
[1,2,3]Department of Computer Science & Engineering,
University Institute of Engineering & Technology (U.I.E.T),
Kurukshetra University Kurukshetra (K.U.K), Haryana, India

Abstract*: Steganography or Stego as it is often referred to in the IT community, literally means, "covered writing" which is derivative from the Greek language. The term Steganography is defined as the art and science of communicating in a mode which hides the subsistence of the communication. And in contrast to Cryptography; where the enemy is allowed to detect; intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem; the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present. It is a budding area which is used for protected data transmission over any public medium. This is a study of novel approach of image Steganography based on LSB (Least Significant Bit) insertion and cryptography technique for the lossless jpeg images has been proposed. The paper discusses an application which ranks images in a user's library based on their suitability as cover objects for some data. Then data is matched to an image so there is less chance of an attacker being able to use steganalysis to recover the data. Therefore application first encrypts the data using cryptography. The message bits are then embedded into an image using Least Significant Bit insertion technique.*
Keywords*: Cryptography, Stegnography, LSB.*

I. Introduction

Cryptography is the art of changing the plain text (Original message) to Cipher text by using the key value. It hides the contents of a secret message from a malicious people. In cryptography the content of the message alone is kept covert, the existence of the message is not kept secret at all. The structure of a message is scrambled to make it meaningless. While seeing this meaningless information hackers came to know the existence of the message. Thus system is broken when the attacker can read the secret message. Data hiding conceals the existence of secret messages while cryptography protects the content of message. The word Steganography comes from the Greek *Steganos*; which mean covered or secret and *graphy* mean writing or drawing i.e., the art of hiding information in ways that prevent detection. Steganography is the process of hiding a secret message within another message. The Steganography can be an invaluable tool in maintaining discretion, which is based on the computer security, veracity and availability. The 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.The Steganography and cryptography differ in the way they are evaluated: The disciplines that study techniques for deciphering cipher messages and detecting hide messages are called *cryptanalysis* and *steganalysis*. Steganography technique is not a new technique. They are some older practices in message hiding such as invisible ink, tiny pin punctures on selected characters and pencil mark on typewritten characters. In term of the key management, Steganography is more secure than cryptography. If the goal of Steganography is to hide secret message into the cover image and it generates the stego-image. The goal of Steganography is to avoid drawing suspicion to the existence of a hidden message. The approach of information hiding technique has recently become important in a number of application areas. The digital audio; video; and pictures are increasingly furnished with distinguishing but imperceptible symbols, which may enclose a hiding copyright notice or serial number or even help to avert unauthorized copying openly. Reversible image has the ability to reconstruct the secret information from the cover image without losing of any information to both cover images as well as to the secret data. In a basic steganographic model, the message M is the secret data that the Sender wishes to hide without any suspicion. Therefore secret message can be audio; video; image; text. The cover X is the original figure; audio file; video file; in which the secret message M is to be embedded. The cover X is also called as "Message Wrapper". It is not necessary that the cover X and the message M should have homogeneous structure. Take example; text message or an audio file can also be hidden into video or image. The cover X and Message M are images.

II. Literature Review

Many research papers have been surveyed for studying the various concepts associated with the Steganography. This section describes the relevant papers of different authors. Ki-Hyun Jung *et al.* [1] in 2014 proposed Steganography is the method of hiding secret data in other data; such as video or an image. The reversible message hiding method can extract the cover image from a stego-image without distortion after extracting the hidden data. This is a paper in which semi-reversible data hiding method that utilizes interpolation and the least significant substitution technique is proposed. The First interpolation method is used to scale up and down the cover image before hiding secret data for a higher capacity and quality. Then secondly; the LSB substitution method is used to embed secret data. Thus experimental results show that the proposed method can embed a large amount of secret data while keeping very high visual quality; where the PSNR is guaranteed to be 37.54 dB (k=3) and 43.94 dB (k=2). Sidham Abhilash *et al.* [2] in 2013 proposed a Novel Lossless Robust Reversible Steganography Method for Copyright Protection of Images. Robust reversible Steganography (RRS) methods are popular in multimedia for protecting copyright; while preserving intactness of host images and providing robustness against unintentional attacks. However, conventional RRS methods are not readily applicable in practice. This is the mainly because I) they fail to offer satisfactory reversibility on large-scale image datasets; II) they have limited robustness in extracting message from the stego images destroyed by different unintentional attacks; and III) some of them suffer from extremely poor invisibility for stego images. There-fore, it is necessary to have a framework to address these three problems; and further improve its performance. The papers present a novel pragmatic framework; wavelet-domain statistical quantity histogram shifting and clustering (WSQH-SC). Compared with conventional methods; WSQH-SC ingeniously constructs new watermark embedding and extraction procedures by histogram shifting and clustering; which are important for improving robustness and reducing run-time complexity. The additionally WSQH-SC includes the property-inspired pixel adjustment to effectively handle overflow and underflow of pixels which results in satisfactory reversibility and invisibility. Furthermore, to increase its practical applicability, WSQH-SC designs an enhanced pixel-wise masking to balance robustness and invisibility. To perform extensive experiments over natural; medical; and synthetic aperture radar images to show the effectiveness of WSQH-SC by comparing with the histogram rotation-based and histogram distribution constrained methods.

Yadav Pooja *et al.* [3] proposed Need of hiding information from intruders has been around since ancient times. In modern digital media is getting advanced like text; image; audio; video etc. Then to maintain the secrecy of information; different methods of hiding have been evolved. Thus one of them is Steganography; which means hiding information under some other information without noticeable change in cover information. The recently Video Steganography has become a boon for providing large amount of data to be transferred secretly. Videos simply a sequence of images; hence much space is available in between for hiding information. the proposed scheme video Steganography is used to hide a secret video stream in cover video stream. The each frame of secret video will be broken into individual components then converted into 8-bit binary values; and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. Therefore to increase more security each bit of secret frame will be stored in cover frames following a pattern BGRRGBGR. Tao Zhang *et al.* [4] proposed new steganalytic method based on statistical distribution of pixel differences, which is designed to detect the presence of spatial LSB matching Steganography in high-resolution natural images. The paper established a statistical model for the distribution of pixel differences in natural images based on the Laplacian distribution and estimates the number of zero pixel difference values based on the number of non-zero pixel difference values according to the characteristics of LSB matching Steganography. Then estimated error is used as distinguishing feature for Steganography classification. Thus experimental results show that the proposed method exhibits excellent performance for the detection of LSB matching Steganography in high-resolution images. It has a low computational complexity and fast computational speed.

Balaji *et al.* [5] proposed Video Steganography is the process of hiding some secret information inside a video. Then addition of this information to the video is not recognizable by the human eye as the change of a pixel color is negligible. Thus paper aims to provide efficient and more secure methods to video Steganography. Then proposed method creates an index for the secret information and the index is placed in a frame of the video itself. To help of this index; the frames containing the secret information are located. Moon *et al.* [6] proposed video as cover media for hiding the secret message and used computer forensics as tool for authentication. To aim is to hide an figure and text behind a video file. To suitable algorithm such as 1LSB; 2LSB; 4LSB is used and 4LSB method found to be good for hiding more secret information data. Thus this paper deal with the idea of video Steganography; and cryptography; the use of computer forensic techniques in both investigative and security manner. Moreover, Bhautmage *et al.* [7] Proposed Data embedding is the process of embedding information in a data source without changing its perceptual quality. Many constraints affect this process: the quantity of data to be hidden; the need for invariance of these data under the conditions where a host signal is subject to distortions such as lossy compression and the degree to which the data must be immune to interception; modification or removal by a third party. A new technique is proposed in this paper for data

embedding and extraction for high resolution AVI videos. In this method instead of changing the LSB of the cover file, the LSB and LSB+3 bits are changed in alternate bytes of the cover file. The secret message is encrypted by using a simple bit exchange method before the actual embedding process starts. An index can also be created for the secret information and the index is placed in a frame of the video itself. To the help of this index; can easily extract the secret message; which can reduce the extraction time. The different techniques and advantages of video Steganography are also discussed in this research paper.

III. Proposed System

A message is plaintext (sometimes called clear text). Then process of disguising a message in such a way as to hide its substance is encryption. Thus an encrypted data is cipher text. Then process of turning cipher text back into plaintext is decryption. It is shown in figure 1 (If you want to follow the ISO 7498-2 standard, use the terms "encipher" and "decipher." It seems that some cultures find the terms "encrypt" and "decrypt" offensive; as they refer to dead bodies). The art and science of keeping messages secure is cryptography; and it is practiced by cryptographers. The cryptanalysts are practitioners of cryptanalysis; the art and science of breaking cipher text; that is; seeing through the disguise. This branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. The modern cryptologists are generally trained in theoretical mathematics—they have to be.

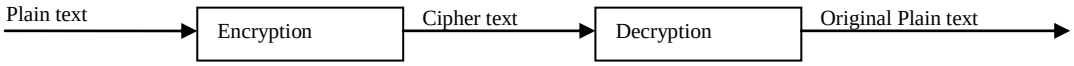

Figure 1.1 Encryption and Decryption

Plaintext is denoted by *M* for message or *P* for plaintext. This can be a stream of bits; a text file; a bitmap; a stream of digitized voice; a digital video image. The computer is concerned; *M* is simply binary data. Then plaintext can be intended for either transmission or storage. The any case *M* is the message to be encrypted. Cipher text is denoted by *C*. It is also binary data: sometimes the same size as *M*; sometimes larger. (Then by combining encryption with compression; *C* may be smaller than *M*. Thus encryption does not accomplish this.)

Then encryption function *E*; operates on *M* to produce *C*. In mathematical notation
$E(M) = C$
In the reverse process, the decryption function *D* operates on *C* to produce *M*:
$D(C) = M$
Then whole point of encrypting and then decrypting a message is to recover the original plaintext; the following identity must hold true:
$D(E(M)) = M$
At last in addition to providing confidentiality; cryptography is often asked to do other jobs:

— *Authentication*: It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else.
— *Integrity*: It should be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one.

— *Non-repudiation*: A sender should not be able to falsely deny later that he sent a message.
These are vital requirements for social interaction on computers; and are analogous to face-to-face interactions. The someone is who he says he is that someone's credentials—whether a driver's license; a medical degree; or a passport—are valid that a document purporting to come from a person actually came from that person. And these are the things that authentication; integrity; and non-repudiation provide. There are many cryptographic algorithms. This is three of the most common:

— *DES (Data Encryption Standard):* It is the most popular computer encryption algorithm. The DES is a U.S. and international standard. This is a symmetric algorithm same the key is used for encryption and decryption.
— *RSA (named for its creators—Rivest; Shamir; and Adleman)*: It is the most accepted public-key algorithm. It can be used for both encryption as well as digital signatures.

— *DSA (Digital Signature Algorithm*): It is used as part of the Digital Signature Standard) is another public-key algorithm. It cannot be used for encryption; but only for digital signatures.
The following are the vital layouts of the projected scheme.

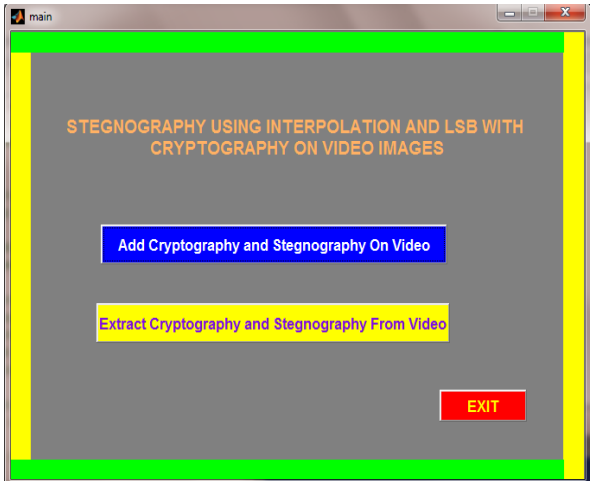

Figure 2. The basic layout of the proposed system.

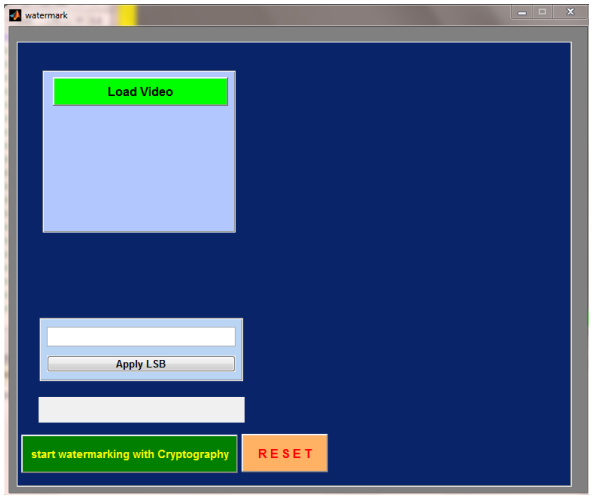

Figure 3. Load the input video.

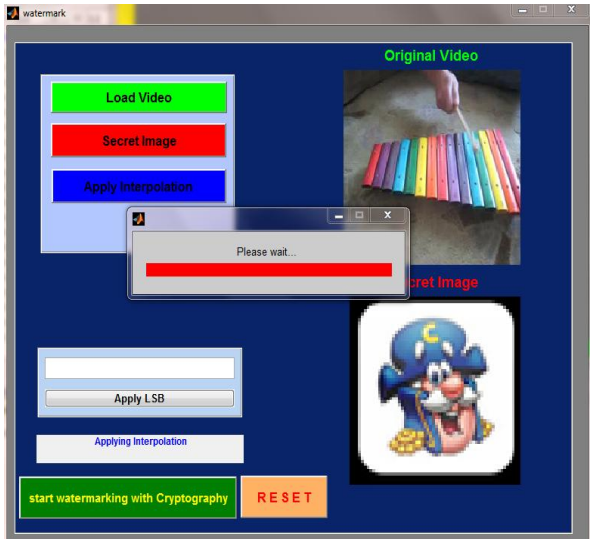

Figure 4. Load the secret image and after that apply the interpolation.

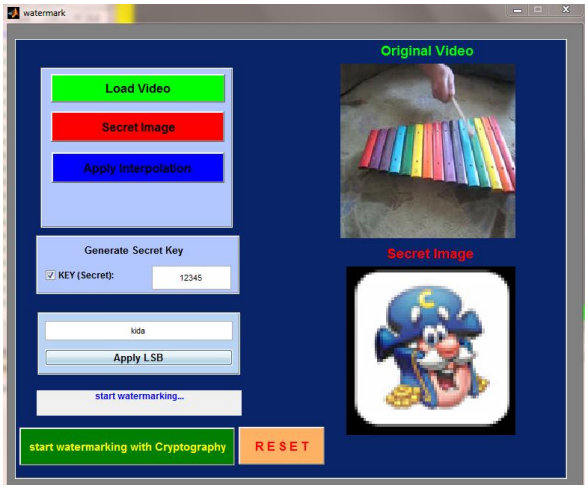

Figure 5. The secret key is been generated.

Figure 6. The layout of the cryptography process.

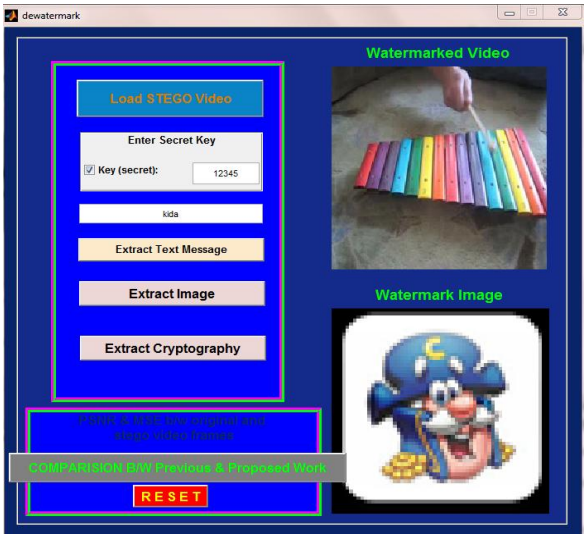

Figure 7. The original image is been extracted.

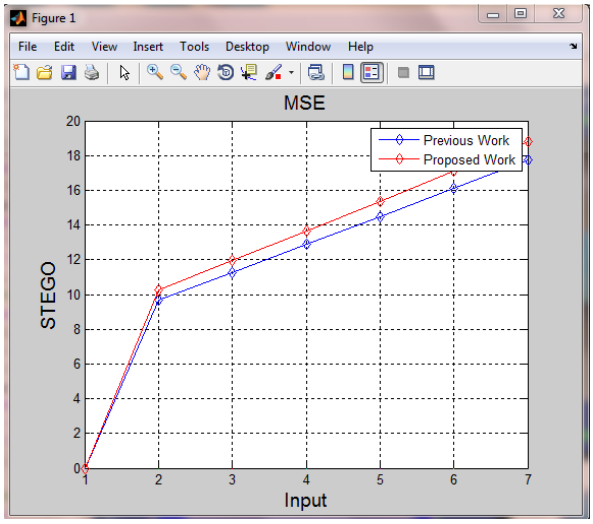

Figure 8. The graphical representation of the proposed system.

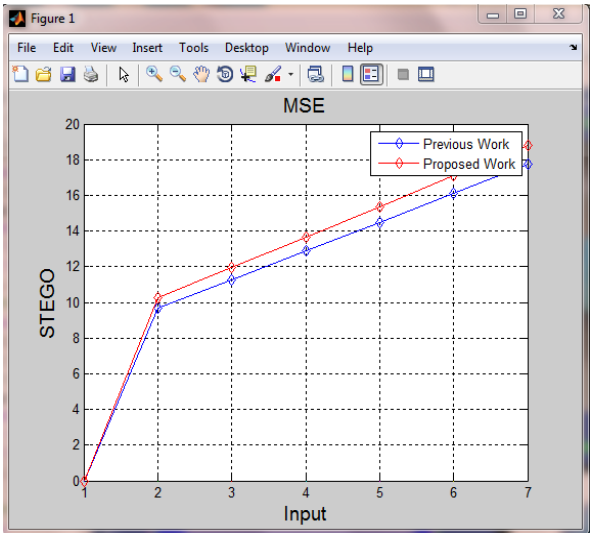

Figure 9. The graphical representation between the previous and the proposed system.

IV. Conclusions

The Steganography has its place in the security. Thus on its own; it won't serve much but when used as a layer of cryptography; it would lead to a greater security. Although only some of the main image steganographic techniques were discussed in this paper; one can see that there exists a large selection of approaches to hiding information in images. Then all the major image file formats have different methods of hiding messages; with different strong and weak points respectively. And where one technique lacks in payload capacity; the other lacks in robustness. Steganography, especially combined with cryptography is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. Then proposed method provides acceptable image quality with very little distortion in the image. The main advantage of this System is to provide high security for key information exchanging. It is also useful in communications for codes self error correction. This can embed corrective audio or image data in case corruption occurs due to poor connection or transmission

References

[1] Awrangjeb M (2003) An overview of reversible data hiding. ICCIT 75–79.

[2] Celik MU, Sharman G, Tekalp AM & Saber E (2002) Reversible data hiding, Proceedings of IEEE 2002International Conference on Image Processing 2, 157–160.

[3] Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recognition 37:469–474.

[4] Chang CC, Lin MH, Hu YC (2002) A fast and secure image hiding scheme based on LSB substitution. Int Pattern Recog 16(4):399–416.

[5] GoljanM, Fredrich F & Du R (2001) Distortion-free data embedding, Proceedings of 4th Information Hiding Workshop, 27–41.

[6] Huang LC, Tseng LY, Hwang MS (2013) A reversible data hiding method by histogram shifting in high quality medical images. J Syst Software 86:716–727

[7] Johnson NF & Jajodia S (1998) Exploring Steganography: seeing the unseen. Comput Pract 26–34.

[8] Jung KH, Yoo KY (2009) Data hiding method using image interpolation. Comput Standards Interfaces 31:465–470.

[9] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001.

[10] Hameed A. Younis, Dr. Turki Y. Abdalla, Dr. Abdulkareem Y. Abdalla , " A Modified Technique For Image Encryption ",online access.

[11] Simmons, G. J. The prisoners' problem and the subliminal channel. In Advances in Cryptology: Proceedings of Crypto 83, pages 51–67. Plenum Press.

[12] Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. In Proc. 4th Int'l Workshop Information Hiding, pages 289–302.2001.