A Review on Data Hiding in Steganography

Harsimranjeet Kaur[1] Er Gurdeep Kaur[2]
[1]Research Fellow [2]Assistant Professor
[1]Desh Bhagat University, Mandi Gobindgarh, Punjab

Abstract— The Internet as a whole does not use secure links, thus information in transit may be vulnerable to interception as well. The importance of reducing a chance of the information being detected during the transmission is being an issue now days. Steganography is the art or practice of concealing a message, image, or file within another message, image, or file. The word Steganography is of Greek origin and means "covered writing" or "concealed writing". Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganography coding inside of a transport layer, such as a document file, image file, program or protocol. There are various number of techniques available for steganography. In our work we have used MD5 and DES for data encryption then MLSB technique will be used for embedding data into the cover image that will turn out to be a stego image that is how we are going to save our data from third party interception. Finally, results are compared in terms of PSNR, MSE with the implementation of Cryptography Technique.

Key words: MD5, DES, PSNR, MSE

I. INTRODUCTION

The translation of data into a unique code. Encryption is the most effective way for data security. To read an encrypted file, you must have authority to a secret password that enables you to *decrypt* it. Without encryption data is called *plain text ;* with encryption data is referred to as *cipher text*.

Data encryption is the act of transfering electronic information into an private state by using algorithms or ciphers. Originally, mainly data encryption was used for passing government and military information electronically. Over time as the public has begun to enter and transmit sensitive information over the internet, data encryption has become more important now these days. Now a days technology is very advance so web browsers will automatically change text when connecting to a secure server. You can tell you are on a secure, encrypted website when the URL start with "https", meaning Hypertext Transmission Protocol, Secure. It's all happen automatically in all cases.

Cryptography is the technique of technologies for hiding information. It tries to hide, encrypt, the information in such a way that a third party who has authority to the hidden, encrypted, data cannot reconstruct, decrypt, the original information. In more practical terms, the encryption methods only apply a certain routine to information so that it's no longer recognizable as its original. With the right key, which was finding before encrypting the data and the accompanying routine for decrypting the information, we can recover the original information. Cryptography was first pioneered many centuries ago. It was the work of specialists to create encryption routines in a large number for the government mainly. Cryptography remained something mainly for the military or government for quite long. Up until a century ago almost entirely and only in the last many years has it become main stream. Now these days it's being used all around us; in ATM cards, on ecommerce websites, for the distribution of copyrighted music and film and mostly in all the applications used today in it world. This is all possible due to the rise of the computer in day by day and readily available gross amounts of computing power. Considering the computing power available nowadays we're actually encrypting very little and leaving the door right open to a lot of sensitive data.

A. How do I know my online information is encrypted?

To make sure any information you enter online is encrypted we offer Data Mask by AOL which will always work silently in the background of your pc's. It scrambles the information you enter online, including log in usernames and passwords, as well as blocks third parties from taking screen captures of what is show on your monitor.

B. Why do we need to encrypt more?

If you don't all ready know it, without encryption you cant put private your data. At least not for your data. It's all in encrypted form like in 1′s and 0′s but doesn't take a genius at all to recognize the data it represents if it's not encrypted when intercepted. And there are thousands of ways to intercept data, i want to tell u some common ways.

- Internet
  is probably the most unsecure place for your data as concerned with privacy. If you don't use a encrypted connection with the server, pretty much anybody can trace their hands on your full communication. People in your local network, your internet provider, the host of the web-site you're visiting, proxies you're tunnel through even if they are transparent and you don't even notice or know, any carrier of your traffic which can be pretty much any arbitrary person for all you know because routes are not chosen statically and you have very little to no influence on that and last but not least someone who specifically targets your communication mostly being a hacker
- E-mail is also same as the internet.
- Instant-messaging is also just as unsecure as the whole rest of the internet!
- WiFi is a special case all by itself. Special for the fact that it's extremely unsecure. This is because the information is just put straight into the air for anybody to receive. With the right antenna this can even be from quite far away.

Further away than you can be from the access point. Can you imagine what can be happens if this is unencrypted, or encrypted with some unsecure encryption such as wep?

- USB-sticks might get stolen or lost. Just use plug 'm in, thanks to plug 'n play, no problem. The average grandmother can do that. Even encrypted

and supposedly safe USB sticks might very well turn out to be very dangerous after all.

- External-hard-drives also suffer from same issues as USB-sticks except for that less of them are out there who actually try and secure your data.
- Personal-Computers
  get stolen. But a bigger risk might be that all the peoples use them as well. May be you don't get fear from your husband, wife or maybe even the kids wandering around through your computer, but what you think about the your friends and your family who visit your house. Maybe even friends of friends during a party? And did you ever think about the possibility that you might ever become under criminal or tax fraud investigation. You don't even have to be feel guilty to be investigated, that's the 'beauty'. But then you say, I've got my account secure with a password and I've made my files secure, isn't that enough? NO! All though it will prevent the occasional authority to access to your files it won't stop the more determent of mind. If they have full authority to the hardware, e.g. stolen computer or you're under investigation, then it's very easy, but even with limited access it's possible. Some years ago at a institution we were able to see a very password from a machine with a padlock on the case, the HDD as only boot device and bios password set. And then there still is the malware that endangers your data.
- Laptops and PC'sboth are same except for that they are stolen much easier, more often, get in the range of different people more easily and that customs have the right to search them if you travel abroad.

II. Types Of Encryption

We have two categories of encryption. One is the symmetric system and the other is the asymmetric system. The following is a simple scenerio to help explain the difference.

Imagine two people, A and B, sending a secret message through the public mail. In this example, A has the secret message and wants to send it to B, after which B sends a secret reply.

A. Private key system

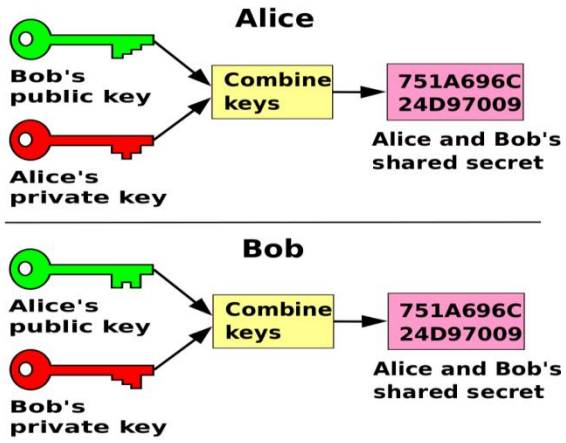

Fig. 1: Private key

A first puts the secret message in a box, and then locks the box using a padlock to which she has a key. She then sends the box to B through regular mail. When B receives the box, he uses an identical copy of A's key to open the box, and reads the message. B can then use the same padlock to send his secret reply.

B. Public-key cryptography

Fig. 2: Public key

In an asymmetric key system (public key system), B and A have separate padlocks. First, A asks B to send his open padlock to her through regular mail, keeping his key to himself. When A receives it she uses it to lock a box containing her message, and sends the locked box to B. B can then unlock the box with his key and read the message from Alice. To reply, B must similarly get Alice's open padlock to lock the box before sending it back to her.

The critical BENEFITS in an asymmetric key system is that B and Alice never need send a copy of their keys to each other. This substantially reduces the chance that a third party will copy a key while it is in transit, allowing said third party to spy on all future messages sent between Alice and Bob. In addition, if B were to be careless and allow someone else to copy *his* key, A's messages to B will be compromised, but A's messages to other people would remain secret, since the other people would be providing different padlocks for Alice to use.

From this story you can see that encryption was created to secures the messages that are sent between two or more parties. There are many different programs that are available to help a technology user to encrypt and secure those messages sent and received.

Examples of symmetric (private key) techniques include:

- RC6
- Two Fish
- Mars
- Irondale
- Blowfish
- Idea
- Gost
- Cast256
- Cast128
- Misty1

C. RSA

RSA is a public key algorithm invented by Rivest, Shamir and Adleman. The key used for encryption is different from the key used for decryption. The algorithm is based on modular exponentiation. Numbers e, d and N are chosen with the property that if A is a number less than N, where d mod N = A. This means that you can encrypt A with e and

decrypt using d. o the other hand you can encrypt using d and decrypt using e.

- The pair of numbers (e, N) is known as the public key and can be unsecure.
- The pair of numbers (d, N) is known as the private key and must be kept secure.

The number e is known as the public exponent, the number d is known as the private exponent, and N is known as the modulus. When talking of key lengths with RSA, what is meant is the modulus length. An algorithm that uses different keys for encryption and decryption is said to be asymmetric. Anybody knowing the public key can use it to create encrypted messages, but only the owner of the secret key can decrypt them.

On the other hand0 the owner of the secret key can encrypt messages that can be decrypted by anybody with the public(about which everyone know) key. Anybody successfully decrypting such messages can be sure that only the owner of the secret key could have encrypted them.

This fact is based upon the digital signature technique. Without going into detail about how e, d and N are related, d can be deduced from e and N if the factors of N can be calculated. Therefore the security of RSA depends on the difficulty of factorizing N. Because factorization is believed to be a hard problem, the longer N is, the more secure the crypto system. Given the power of modern computers, a length of 768 bits is considered reasonably safe, but for serious commercial use 1024 bits is calculated. The problem with choosing long keys is that RSA is very slow compared with a symmetric block cipher such as DES, and the longer the key the slower it is. The better solution is to use RSA for digital signatures and for protecting DES keys. Bulk data encryption can be done using DES.

D. HASH

A 'hash algorithm' is used for computing a condensed representation of a limited length information. Also known as a 'message digest', or a 'fingerprint'..

E. MD5

MD5 is a 128 bit message digest function. It was produced by Ron Rivest. MD5 is a hashing algorithm that takes a message of up to 264 bits and reduces it to a digest of 128 bits The algorithm is a development of the MD4 algorithm produced by Ronald Rivest and announced in 1990. MD4 was flawed, so Rivest made some revisions, and the resulting algorithm was christened MD5. Any hashing algorithm should be such that, given a digest and the correspondence message from which it was derived, it should be computationally not feasible to construct a different message with the same digest.

F. AES

it stands for Advanced Encryption Standard a design principle known as a substitution-permutation network, and is fast in both software and hardware. Not like its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a limited block size. i.e 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum.i.e 128 and a maximum of 256 bits. AES operates on a 4×4 column-matrix of bytes, termed the state, some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special limited field. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four same but they are different stages for each other, including one that depends on the encryption key itself. A set of reverse rounds are applied to transfer ciphertext back into the original plaintext using the same encryption key.

G. SHA-1

SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits .Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reason SHA-1 is more preferred to MD5.

H. HMAC

HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

I. Blowfish

Blowfish is a symmetric encryption algorithm, meaning that it uses the one secret key to both encrypt and decrypt of messages. It is also a block cipher, meaning that it divides a message up into limited length blocks during encryption and decryption. The block length for Blowfish is large i.e 64 bits messages that aren't a multiple of eight bytes in size must be padded.

- It has a scalable key, from 32 bits to at least 256 bits.
- Uses a very simple operations that are efficient on microprocessors. e.g. exclusive-or, addition, table lookup, modular- multiplication. this does't use variable-length shifts or bit-wise permutations or conditional jumps.
- Employs pre-computable sub keys. On large-memory systems, these sub keys can be pre-computed for faster operation. Not pre-computing the sub keys will result in slower operation it should still be possible to encrypt data without any pre-computations.
- Only Uses sub keys that are a one-way hash of the key. This allows the use of long passphrases for the key without compromising security.
- Uses only a design that is very simple to understand. This facilitates analysis and increase the confidence in the algorithm. In practice, this means that the algorithm will be a Feistel iterated block cipher.
- Same algorithms use in both the encryption and descrption.
- It uses same Feistel structure of blowfish algorithm but the only difference is Decryption algorithm

takes Cipher text as input and transfer it into original plain text.

III. STEGANOGRAPHY

The first recorded uses of steganography can be traced back to 440 BC when Herodotus mentions two examples in his *Histories*.[3] Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand.

Steganography is an art in which we deal with communication of secret data in an appropriate carrier, e.g., image, audio, video or TCP/IP header file. Steganography's goal is to doest show the very existence of embedded data so as not to arouse an eavesdropper's suspicion. In our work, new encryption scheme is made for hiding private data.

Fig. 3: Stenography

The methodology used in our work is cover image acquisition and then we take the image or text which is to be hidden. After applying algorithms named as Blowfish, RSA and MLSB, we will convert the data in to a secret data. Parameters are calculated for checking the performance like EPI, PSNR, MSE, comparison is also done for checking the performance with last works.

IV. TECHNIQUES OF STENOGRAPHY

Steganography has been widely used, including in recent historical times and the present day. Known examples include:

- Hidden messages within wax tablets — in ancient Greece, people wrote messages on the wood, then covered it with wax upon which an innocent covering message was written.
- Hidden messages on messenger's body — also used in ancient Greece. Herodotus tells the story of a message tattooed on the shaved head of a slave of Histiaeus, hidden by the hair that afterwards grew over it, and exposed by shaving the head again. The message allegedly carried a warning to Greece about Persian invasion plans. This method has obvious drawbacks, such as delayed transmission while waiting for the slave's hair to grow, and the restrictions on the number and size of messages that can be encoded on one person's scalp.
- In the early days of the printing press, it was common to mix different typefaces on a printed page due to the printer not having enough copies of some letters otherwise. Because of this, a message could be hidden using 2 (or more) different typefaces, such as normal or italic.
- During World War II, the French Resistance sent some messages written on the backs of couriers using invisible ink.
- Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages.
- Messages written in Morse code on knitting yarn and then knitted into a piece of clothing worn by a courier.
- Jeremiah Denton repeatedly blinked his eyes in Morse Code during the 1966 televised press conference that he was forced into as an American POW by his North Vietnamese captors, spelling out the word, "T-O-R-T-U-R-E". This confirmed for the first time to the U.S. Military (naval intelligence) and Americans that American POWs were being tortured in North Vietnam.
- Messages written on envelopes in the area covered by postage stamps.
- During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute, approximately less than the size of the period produced by a typewriter. World War II microdots needed to be embedded in the paper and covered with an adhesive, such as collodion. This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards.
- During WWII, Velvalee Dickinson, a spy for Japan in New York City, sent information to accommodation addresses in neutral South America. She was a dealer in dolls, and her letters discussed the quantity and type of doll to ship. The stegotext was the doll orders, while the concealed "plaintext" was itself encoded and gave information about ship movements, etc. Her case became somewhat famous and she became known as the Doll Woman.
- Cold War counter-propaganda. In 1968, crew members of the USS *Pueblo* intelligence ship held as prisoners by North Korea, communicated in sign language during staged photo opportunities, informing the United States they were not defectors, but were captives of the North Koreans. In other photos presented to the US, crew members gave "the finger" to the unsuspecting North Koreans, in an attempt to discredit photos that showed them smiling and comfortable.

V. DIFFERENT KINDS OF STEGANOGRAPHY

Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". As defined by steganography is the art and science of

communicating in such a way that the presence of a any message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but now technology become very advance so we can find so many techniques of stenography.. Steganography can be split into two types, these are Fragile and Robust. The following section describes the definition of these two different types of steganography.

all digital file formats can be used for steganography, but the formats that are more suitable are those with a large degree of redundancy. Redundancy can be defined as the bits of an object that give accuracy far greater than necessary for the object's use and display [14]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files comply with this requirement, while research has also uncovered other file formats that can be used for information hiding.

A. LSB

LSB steganography is the very simplest steganographic techniques, which embeds sprivate messages in a subset of the LSB plane of the image. A large number of popular steganographic tools, and techniques such as S-Tools 4, Steganos and StegoDos, are based on LSB replacement in the spatial domain. Private messages can be embedded in LSB plane by sequential or random LSB replacement. Sequential.LSB replacement can be implemented more conveniently but has a much serious privacy problem in that there is an obvious statistical difference between the modified part and the unmodified part of the stego-image. By random LSB replacement secret messages can be randomly scattered in stego-images, so the steganographic privacy is improved.

B. Transform Domain Technique

In this tecnnique; the secret message is embedded in the transform space of the cover. An example of this method includes the Discrete Cosine Transform (DCT) domain. The cover image is split into 8*8 blocks and every block is used to encode one message bit. The blocks are chosen in a pseudorandom manner. The size of two predefined DCT coefficients is modulated using the message bit. The two coefficients are choose from middle frequencies.

C. Spread Spectrum Technique

This technique uses the concept of spread spectrum. The message is spread over a wide frequency bandwidth. The signal to noise ratio in every frequency band is so small that it is very much difficult to detect. Even if parts of message are erased from several bands, enough information is present in other bands to recover the information. Thus it is difficult to erased the message completely without entirely destroying the cover .It is a very rough technique that finds application in military communication.

D. Statistical Techniques

In these techniques, the information is encoded by changing several properties of the cover. The cover is convert into blocks and each block is used to hide one message bit .If the message bit is one, then the cover block is modified otherwise the cover block is not modified. This technique is difficult to apply because a good test must be found that allows for proper distinction between modified and unmodified cover blocks.

E. Distortion Techniques

The information is stored by distorting the signal. The encoder applies a sequence of modifications to the cover. This sequence corresponds to the secret message. The decoder measures the differences between both the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message. This method is used only in some applications because the decoder must have access to the original cover.

Steganography in Digital Mediums Depending on the type of the cover object there are so many beneficial steganographic techniques which are followed in order to obtain n security.

This paper introduced various stegnography techniques for hiding data in images. The images are show with numerical values of each pixel where the value represents the color and intensity of the each pixel.

There are mainly of two types of Images 8-bit images, 24-bit images

1) Image Steganography

Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the important data.

Both in International Journal of Advanced Science and Technology Network Steganography:

When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields.

2) Video Steganography

Video Steganography is a technique to hide any kind of information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g.,8.667 to 9) which is used to hide the important data in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

3) Audio Steganography

When taking audio as a carrier for information hiding it is called audio steganography. It has become very important medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc

4) Text Steganography

General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code and etcis used to find formation Hiding.

VI. MD5 (MESSAGE-DIGEST ALGORITHM 5)

MD5 (Message-Digest algorithm 5) is a well-known cryptographic hash function with a 128-bit resulting hash value. MD5 is widely used in security-related applications, and is also frequently used to check the integrity of files. The MD5 value of file is considered to be a highly reliable fingerprint that can be used to verify the integrity of the file's contents. If as little as a single bit value in the file is modified, the MD5 value for the file will completely change. Forgery of a file in a way that causes MD5 to

generate the same result as that for the original file is considered to be extremely difficult.The set of MD5 checksums for critical system, application, and data files provides a compact way to store information for use during periodic integrity checks of those files.Details for the MD5 cryptographic hash algorithm and C source code are provided in RFC 1321. The MD5 algorithm has been implemented in numerous computer languages including C, Perl, and Java.Algorithm Design In MD5, the input message is broken up into chunks of 512-bit blocks (each with sixteen 32-bit sub-blocks). After a series of operations, MD5 produces a 128-bit message digest with four concatenated 32-bit blocks for the integrity of a file. To compute the digest of a message, padding bits are appended first to make the message's length congruent to 448, modulo 512, and then the length bits. A 64-bit portion is appended to indicate the length of the actual message.MD5 algorithm operates on a 128-bit state which is divided into four 32-bit words (denoted as A, B, C and D) and initialized. Each 512-bit message block is applied in turn to modify the state. The processing of a message block consists of four similar rounds, each of which is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. At last, MD5's output is produced by cascading A, B, C and D after the final round.

VII. MD5 Collisions

Hash function is a useful cryptographic tool which should satisfy several requirements to keep it robust and secure on encryption. One of these requirements is collision resistance, i.e., it is hard to compute messages m and m0 where m6=m0and yet H(m) =H(m0). A hash function is claimed good

if it is extremely difficult to find such existing pairs. MD5is an encryption-based hash function and suffers a crucial weakness of collision. Finding a collision by a brute force attack requires at most2128 applications of MD5 and2 64 by the birthday paradox, since MD5 has 128-bit hash.

Early in 1993, Bert den Boer and Antoon Bosselaers [1] discovered the first pseudo-collision of MD5. In 1996, H. Dobbertin announced a collision of the compression function of MD5 [6]. In 2004 when Xiaoyun Wang and Hongbo Yupresented a collision for MD5 with two input blocks in less than an hour and 5 minutes on a IBM P690 [2]. In 2006,

Vlastimil Klima published an algorithm [7] to find a collision within one minute on a single notebook computer, using a "tunneling" method. All these different attacks on MD5 were constructed through multi-block collision method. Tao Xie and Dengguo Feng announced the first single-block MD5collision (two 64-byte messages with the same MD5 hash) in 2010 [8]. MD5 is recommended to be replaced by some other alternative methods such as SHA-1 and SHA-2, to keep it safe in application

VIII. Data Encryption Standard

The Data Encryption Standard (DES) is a previously predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. The publication of an NSA-approved encryption standard simultaneously resulted in its quick international adoption and widespread academic scrutiny. Controversies arose out of classified design elements, a relatively short key length of the symmetric-key block cipher design, and the involvement of the NSA, nourishing suspicions about a backdoor. The intense academic scrutiny the algorithm received over time led to the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; in January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes (see chronology). There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology (formerly the National Bureau of Standards).

IX. Conclusion

Data hiding is the most striking feature in security / Internet communications. This study started by carrying out a comprehensive systematic review on research papers of Image Steganography and Cryptography techniques. The review was basically designed as summarize the existing findings, to identify gaps in existing research and to find potential for improvement. The survey shows that the research on security in internet communication through hiding data in images has made much progress in the recent years. Many different approaches have been revised with different strengths and weaknesses. All these techniques will be used for getting more security in the data. By doing these techniques the data is hidden in the image will be very difficult for the third party to extract.we are trying to achieve more security in the data.

References

[1] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., "Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[2] Bailey, K., and Curran, K., 2006. "An evaluation of image based steganography methods", Journal of

Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88.

[3] Behera, S.K., Swarup, M.A., and Mohamed, A.K., 2010. "Colour Guided Colour Image Steganography", Universal Journal of Computer Science and Engineering Technology, Vol. 1, No. 1, pp. 16-23.

[4] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., 2007. " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194.

[5] Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" found online at http://www.nicetext.com/doc/isc01.pdf.

[6] Dai, Y., Liu, G., and WangBreaking, Z., 2006. "Predictive-Coding- Based Steganography and Modification for Enhanced Security", IJCSNS International Journal of Computer Science and Network Security, Vol. 6, No. 3b, pp. - 329-333.

[7] Gutub, A., Al-Qahtani, A., and Tabakh, A., 2009. "Triple-A: Secure RGB image steganography based on randomization", Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 – 403.

[8] Gutub, A.A.A., et al., 2010. "Pixel Indicator Technique for RGB Image Steganography", Journal Of Emerging Technologies In Web Intelligence, Vol. 2, No.1, pp. 193-198.

[9] Gutub, A., Mahmoud, A., Muhammad A.-G., Shaheen, A., and Alvi, A., 2008. "Pixel Indicator High Capacity Technique for RGB Image Based Steganography", WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, U.A.E., pp. 154-159.

[10] Hussain, M., et al, 2010. "Pixel intensity based high capacity data embedding method",Information and Emerging Technologies (ICIET), International Conference, pp. 1 – 5.

