Information Hiding using Tiny Encryption Algorithm Steganography on Video

Ashok Kumar Yadav[1], Ramnaresh[2], Kamaldeep Joshi[3], Abhijeet Mahey[4], Abhishek Kumar[5], Kumar Sheetanshu[6], Pankaj Gupta[7]
[1,2,4,5,6,7]*Amity School of Engineering and Technology, New Delhi, India*
[3]*Maharishi Dayanand University, Haryana, India*

Abstract- Steganography and cryptography can provide information security, but each has their own concerns. Issue with cryptography is that it is not sufficient in itself and issue with steganography is that, when the plausible deniability uncovered or even suspected, at that point the information is undermined. This paper presents a consolidated method for information security utilizing cryptography and steganography procedures to improve the security of the data. Initially, the Tiny Encryption Algorithm (TEA) is utilized to encode the information. Furthermore, the scrambled message is shrouded utilizing steganography strategy. In this way, two dimensions of security have been proposed utilizing a half and half procedure. The proposed procedure gives high inserting capacity and astounding documents post installing.

Keywords - Steganography; PVD (Pixel Value Difference); Encryption; Decryption; Tiny Encryption Algorithm (TEA)

I. INTRODUCTION

Transferring data through web may have expose individual information which might be hacked by man-in-the-middle attack (MITM) assaults. The nodes usually require secure and private and interchanges for some reasons, for example, to conceal their classified data from assailants while using an open channel. The secrecy and information security are required to protect against unapproved access and use of information. Likewise, there are large numbers of applications on the internet that requires clients to fill frames that use individual data, for example, phone numbers, addresses, and advanced installment statistics. So information security becomes increasingly significant [1]. Cryptography and steganography are the regular techniques for verifying records or date in a correspondence [2-4]. The term cryptography finds its origin in the Greek word "kryptós" meaning "covered up" and "gràphin" meaning "composing" [2-4]. In this way, correct significance of cryptography is "shrouded composing". Cryptography is a specialty of using scientific means to decode and scramble information to keep information verified by altering comprehensible information structure (plain-content) into ambiguous structure (figure content). Any cryptosystem consist of encryption calculation, plain-content, decoding calculation, Ciphered content, and Key to unscramble it. Plain-content is information which is in its ordinary, coherent or reasonable structure.

The Key (an alphanumeric blend produced by calculation) is used to control the figure framework, and it is known to the sender and collector [5, 6]. Cryptography is extremely incredible for verifying information; crypto analysis could prevail with regards to breaking the figures by investigating the figure content and with assistance of different instruments recover the plaintext [5].

We can classify cryptographic systems into 3 operations:-

1.1. Operation on Plaintext

There are two kinds of activities that are performed on plain-text to change plain-text to figured content. In the principal task, each part in plain-text (i.e., bit, letters, and congregation of bits or letters) is substituted for each other in the figured content. In these types of methods, a balanced mapping is performed between the components, for example, Caesar figure. While in the second kind of activity, every character in plain-text is replaced with each other dependent on a mapping aimed at by the key. In this, the plain-text characters remain the equivalent however they are revamped into various configurations, for example, Rail Fence figure and so on. Most of frameworks known as item frameworks and these include large number of phases of substitutions and transpositions to make it hard to break.

1.2. Number of Keys Used

If the sender and the beneficiary utilize a similar key to encode and unscramble the information, the framework is known as symmetric, single key, traditional encryption or mystery key. The direct and fast method is symmetric encryption. In the event where the dispatcher and collector utilize distinctive keys (open key and private key) to jumble and decipher the plaintext separately, the framework is known as deviated, two key, or open key encryption.

1.3. Data processing Method

Block figure works on fixed-length gatherings of bits, known as blocks, and creates a yield obstruct for each info square. A stream figure works on each plaintext part consistently, and produces one part at any given moment, as it comes.

The word Steganography comes from the Greek word "steganos" meaning "impervious" and, "grafia" meaning "expressing" characterizing it as "invulnerable composition". Steganography is viewed as the workmanship and exploration of concealing data in other data. There are two basic methods for picture installing in stegnographic system; spatial area and change space.
Our point is to shroud mystery information in the sound and picture of a video document. Video has such a large number of still casings of picture and sound, we can choose any frame for concealing our information.
Steganography framework contains two frameworks, one for inserting and second for extraction. The inserting process includes concealing a mystery message in a envelop media (cover picture), and the aftereffect of installing process is stego picture. Here problem arises because the mystery message won't go without being seen if an outsider attempts to catch the transmitted information (spread picture). The extraction process is exceptionally basic since it is just the reverse of the installing procedure, where the mystery message is extricated toward the end.
For evaluation of the nature of picture, stego picture and cover picture are compared. This requires a proportion of stego-picture quality; generally utilized measures are Mean Square Error (MSE), and Peak Signal-to-Noise Ratio (PSNR). Mean Square Error (MSE) is used to evaluate the distinction between the underlying (spread) and the misshaped or uproarious (Stego) picture.
The steganography methods can be divided into three classes: Public Key Steganography, Secret Key Steganography and Pure Steganography
1) Pure Steganography: Pure steganography is a steganography approach without consolidating different strategies. It conceals the data inside spread transporter.
2) Secret Key Steganography: It uses the mix of the secret key cryptography procedure and the steganography approach. This method of steganography encodes the mystery message by mystery key system and afterward hides the scrambled information inside spread transporter.
3) Public Key Steganography: This method is the blend of the open key cryptography methods and the steganography methods. The possibility of this sort is to scramble the mystery information utilizing the open key methodology and after that shroud the encoded data.

The Difference between Cryptography and Steganography:

- Cryptography hides information in secret or private text in an unintelligible form such that adversaries are unable to read the information or text prevents but Steganography hides the very existence of information (i.e., Cryptography makes data unintelligible while Steganography tends to hides presence of information).
- Cryptography changes the nature of the message while Steganography does not alter the format or content of the message.
- Cryptography is more common technology than Steganography technology.
- Large numbers of the algorithms of Cryptography are well developed, but the algorithms of Steganography are not well known or simply we can say that a lot of work has been done in the field of cryptography while the field of steganography is still relatively new.
- In Cryptography, the robustness of algorithm depends on the complexity of algorithms and mainly on key size. Large key size means more computational capacity is required to decrypt ciphered text, which is expensive. In Steganography, if the presence of the hidden message is detected, the message is compromised.
- Cryptography provides the security by actualizing public and private key(s) with hash functions or validation codes or digital signatures. On the other hand steganography can't give the vast majority of the security destinations (Integrity, legitimacy and non-renouncement) independent from anyone else without utilizing the cryptographic systems. Anyway it gives privacy without anyone else in light of the fact that generally just the concerned individual realizes that the message is covered up in some sort of medium.

In this paper, the Advanced LSB steganography method is utilized to improve protection by utilizing TEA which incorporates methods to encode and shroud the message inside a cover picture. In this manner, if an aggressor questions the stego picture and tries to extract the message from the stego picture, he must require the ways to decode the scrambled information.

The remainder of this paper is composed as pursues; related work will be talked about in second section and the proposed method will be given in third section. At that point exploratory aftereffects of the proposed technique will be given in segment 4. At long last, segment 5 finishes up the paper and future work.

II. TINY ENCRYPTION ALGORITHM (TEA)

TEA is a cryptographic algorithm used for cryptography [7]. TEA reduces the memory usage and boosts speed. It belongs to class of symmetric block cipher. TEA is an improvement to differential cryptanalysis. It accomplishes total dissemination (where a single piece distinction in the plaintext will cause roughly 32 bit contrasts in the figure content) after just six rounds. In this paper we reviewed the most widely a block figure calculation.

The TEA is a symmetric kind cipher that utilizes logarithmic activities. All the bits of information and key are mixed iteratively by tow fold method. The key timetable calculation is basic; 128-piece encryption key K is divided into four 32-bit squares K = (K[0], K[1], K[2], K[3]). Time execution on is exceptionally great in these settings.

In square figure we first enter plain content is entered and then we apply the transformation or round function to change it into the figure content. In Feistel figure the content is scrambled and the encoded content is separated into two parts, one a large portion of the round capacity F, and sub key is connected and the yield of F is exclusive OR (XOR) with other half. At that point swap the two parts. Each round pursues similar strides beside from the last round. In the last round there is no swapping of two parts [5,6].

2.1 Tiny Encryption Algorithm

Step 1. Take $x=V_0$, $y=V_1$ source data to be encrypted
Step 2. Take K_0 to K_3 encoding key
Step 3. Take key constant d=0x9E3779B9
Step 4. Take n=32 and sum=0.
Step 5. Repeat while (n=!0)
    Step 5.1. sum=sum+d
    Step 5.2 $x=x+(y*16+ K_0)$ XOR $(y*+sum)$ XOR $(floor(y/32)+ K_1)$
    Step 5.3 $y=y+(x*16+ K_2)$ XOR $(x+sum)$ XOR $(floor(x/32)+ K_3)$
    Step 5.4 n=n-1
Step 6. $V_0 =x$, $V_1 = y$

2.2 Tiny Decryption Algorithm

Step 1. Take $x=V_0$, $y=V_1$ encrypted source and
Step 2. Take K_0 to K_3 encoding key, $k0= K_0$, $k1= K_1$, $k2= K_2$, $k3= K_3$
Step 3. Take key constant d=0x9E3779B9
Step 4. Take n=32 and sum=0xC6EF3720
Step 5. Repeat while (n=!0)
    Step 5.1. y=y-(x*16+k2) XOR (x+sum) XOR (floor(x/32+k3)
    Step 5.2. x=x-(y*16+k0) XOR (y+sum) XOR (floor(y/32+k1)
    Step 5.3 sum=sum-d
    Step 5.4 n=n-1
Step 6. $V_0 =x$, $V_1 = y$

Working of TEA depends on two 32-bit unsigned whole numbers (from 64-bit information square) and utilizes a 128-piece key. It has a Feistel structure with a planned 64 rounds, normally executed two by two named cycles. It has an amazingly basic key timetable, joining together the bulk of the key material in the same manner for each cycle. Various products of an enchantment steady are utilized to avert straightforward assaults dependent on the symmetry of the rounds. The enchantment consistent, 2654435769 or 0x9E3779B9 is picked to be $\lfloor 232/\phi \rfloor$, where ϕ is the brilliant ratio [7].

There are several shortcomings of TEA. First, it experiences equal keys - each key is proportionate to three others, which means that the powerful size of key is just 126 bits [5]. Accordingly, TEA is mainly useless as a cryptographic hash work. This weakness encouraged a strategy for gaining accessing Microsoft's Xbox game comfort, where the figure was utilized as a hash function. TEA is additionally helpless to a related-key assault which uses 223 picked plaintexts under a related-key pair, with 232 time complexity. XTEA figure was planned to overcome these shortcomings [8].

As the name proposes, the Tiny Encryption Algorithm is little in size. On the whole, it very well may be executed in a couple of lines of programming code. This is significant on the grounds that it implies that it tends to be incorporated into practically any sort of programming bundle, even those with genuine space requirements. For instance, the product on your phone or the product for the GPS in your vehicle. The encryption steps are likewise straightforward, making it easy to execute and keep up.

The process of decryption is same as the encryption process. In the decoding process the cipher text is used as input to the algorithm, but the sub keys K[*i*] are used in the reverse order.

III. STEGANOGRAPHY

Steganography is a craft of concealing one type of information into another type of innocent looking information. Steganography implies mystery composing. Presently multi day's steganography has turned out to be extremely prevalent. It is tied in with covering data from others. As the scrambled information bundle is itself a proof of the presence of important data so steganography is utilized alongside cryptography. Steganography makes the figured content undetectable to unintended clients.

Steganography is process of concealing private or touchy data in carrier such that adversary doesn't know of a secret communication. Steganography is utilized to secure the data that we need to avoid unintended watchers. It includes the way for concealing data so it gives the idea that no secret data is carried by carrier. In the event that an unapproved individual endeavors to block the information, at that point he won't most likely do it as he won't probably observe that information so there will be no endeavor to decode the information.

Steganography is used to hide a document inside other innocent carrier and to send it to the end client. At the point when data is covered up inside a record, the information is normally scrambled with a secret key to make it increasingly secure.

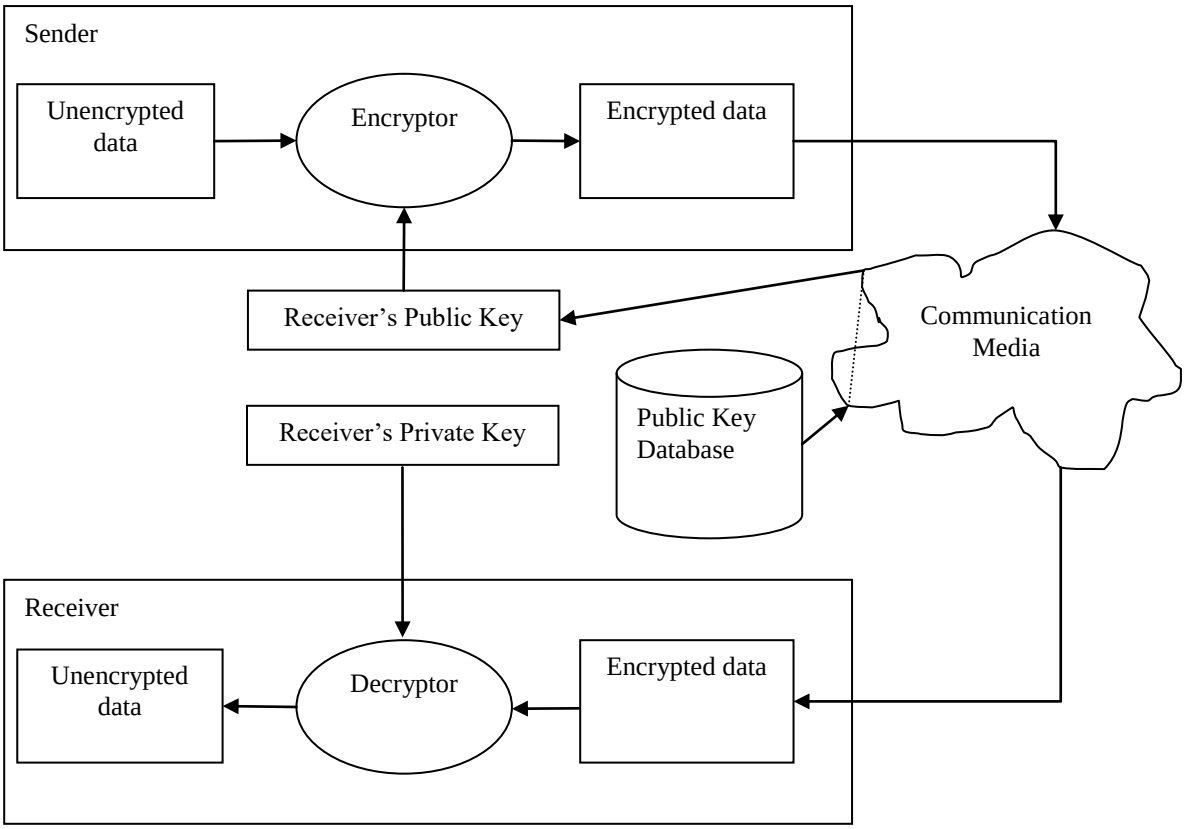

Fig.1 Steganography System

There are large numbers of methods used to hide user information inside the carrier picture, audio or video files. The two most common methods are LSB (Least Significant Byte) and Injection method.

The least significant bit (LSB) algorithm is used in this stego machine to conceal or hide the data in a video file. The advantages of the LSB coding method are low computational complexity and very high watermark channel bit rate. The robustness of LSB can be increased with the LSB depth used for data hiding. The user date is embedded inside carrier by modifying the least significant bits of the carrier file's individual pixels. Three bits of secret information are carried by each pixel, one in each RGB values. Using a 24-bit image, it is possible to hide up to 2,359,296 bits using a 1024x768 pixel image. Date can be hidden from human eyes because human eye cannot easily distinguish 21-bit color from 24-bit.

LSB represents Least Significant piece. The thought behind LSB implanting is that on the off chance that we change the last piece estimation of a pixel, there won't be much unmistakable change in the shading. For instance, 0 is dark. Changing the incentive to 1 won't make a big deal about a distinction since it is as yet dark, only a lighter shade.

The encoding is finished utilizing the accompanying advances:

- Convert the picture to greyscale
- Resize the picture if necessary
- Convert the message to its paired configuration
- Instate yield picture same as info picture
- Cross through every pixel of the picture and do the accompanying:
- Convert the pixel incentive to paired
- Get the following piece of the message to be implanted
- Make a variable temp
- In the event that the message bit and the LSB of the pixel are same, set temp = 0
- In the event that the message bit and the LSB of the pixel are extraordinary, set temp = 1
- This setting of temp should be possible by taking XOR of message bit and the LSB of the pixel
- Update the pixel of yield picture to include picture pixel esteem + temp
- Continue refreshing the yield picture till every one of the bits in the message are implanted
- At long last, compose the contribution just as the yield picture to nearby framework.

IV. ADVANTAGES

- Video quality is carefully saved even after secret the data is embedded.
- Ability to encode and unscramble the information with the pictures in all respects effectively in less measure of time and assets.
- With the utilization of this framework, a picture subsequent to concealing the information won't corrupt in quality.

V. REFERENCES

[1] Sarkar, Anindya, Upamanyu Madhow, Shivkumar Chandrasekaran, and Bangalore S. Manjunath. "Adaptive MPEG-2 video data hiding scheme." In *Security, Steganography, and Watermarking of Multimedia Contents IX*, vol. 6505, p. 65051D. International Society for Optics and Photonics, 2007.

[2] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," *IEEE Computer*,pp. 26-34, February 1998.

[3] A. Gutub, M. Fattani, "A Novel Arabic Text Steganography Method using letter Points and Extension", WASET International Conference on Computer Information and System Science and Engineering (ICCISSE), Vienna, Austria, May 25-27, 2007.

[4] Simmons G. J, "The Prisoners Problem and the Subliminal Channel", *Proceedings of crypto '83*, Plenum Press, pp 51-67, 1983.

[5] Wheeler, David J., and Roger M. Needham. "TEA, a tiny encryption algorithm." In *International Workshop on Fast Software Encryption*, pp. 363-366. Springer, Berlin, Heidelberg, 1994.

[6] Biryukov, Alex, and David Wagner. "Slide attacks." In *International Workshop on Fast Software Encryption*, pp. 245-259. Springer, Berlin, Heidelberg, 1999.

[7] Andem, Vikram Reddy. "A cryptanalysis of the tiny encryption algorithm." PhD diss., University of Alabama, 2003.

[8] Ali M Ahmad, Ghazali Bin Sulong, Mohd.Shafry, B.Mohd.Rahim, Saparudin, "A 2-tier Data Hiding Technique Using Exploiting Modification Direction Method And Huffman Coding", ACEEE Int. J. on Information Technology, Vol. 02, No. 02, April 2012.