National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

A Comparison of Different Data Hiding Techniques

Aditya Gupta[1], Prabal Verma[2], Rakesh Singh Sambyal[3]

[1,2] Department of Computer Science and Engineering, BGSBU, Rajouri. Jammu & Kashmir, India
[3] Department of Information Technology and Engineering, BGSBU, Rajouri, Jammu & Kashmir, India

ABSTRACT

Data or information is exceptionally urgent asset to us. In this manner securing the data turns into all the more fundamental. The transmission through which we send information does not provide a good level of information security, so different techniques for securing information are required. Hiding of this important asset is an exceptionally critical part today. It gave strategies to scrambling the data with the goal that it ends up unintelligible for any unintended client. This paper surveys the methods that exist for hiding of information and by what means can these be consolidated to give another level of security.

Keywords : Steganography,Cryptography,Watermarking

I. INTRODUCTION

Information or data is exceptionally crucial to any association or any distinctive individual. No one of us likes our discussion being caught as it contains the capability of being misused. Same is the circumstance with the data of any affiliation or of any person. The trading of information among two potential groups must be in done in a secured strategy to avoid any changes. Two kinds of problems may exist during the transmission or exchange of crucial information. The unintended user who may attempt to capture this discussion can either mess with this data to change its unique significance or may change or modify its content to make its personal benefit [1]. These two attacks may affect the integrity and confidentiality of the contents of the message being passed from the source to the intended destination. There is a challenging task of avoiding the unintentional access to the information. Information hiding has been in the use for the long time. In the past time the people used to transfer crucial and secret information through hidden images [1].

The data hiding mechanisms come into the picture because of the simple fact that there is no secured or safe way of transmission of data from the source to the intended receiver without being captured by an unintended person. So there is a need of some sort of secured methods so that there is no scope for unintended receiver to capture or modify the original data.

Security Attacks: In earlier days when there were no secured ways were available to protect the data during transmission there was a huge scope of attack on information being transferred between intended users. A security attack is simply an action performed by the unintended user in order to hamper the security of an information which acts as an asset to an organisation. There may be several kinds of attacks which are broadly classified as:

Interruption: This is simply an attack on availability. This type of attacks limits the user from using the resource of an organisation. A simple example of this is cutting of transmission media.

Interception: In this type of attack an eavesdropper or forger simply intercepts the message being passed from source to the intended user so that the value of an information is lost. This type of attack simply focuses on confidentiality. A simple example of this attack is tapping of wire to capture the information.

Modification: In this type of attack, an eavesdropper not only gains access to the information being passed but also modifies the actual content of the message. This type of attack simply focuses on integrity.

Fabrication: In this type of attack, an eavesdropper tries to put fake information into the information being transformed. This type of attack simply focuses on authentication.

II. DATA HIDING TECHNIQUES

Data Hiding Techniques hides the data and make it impossible for unintended user to either capture it or modify it. Several techniques used for hiding the data includes:

Cryptography: The word cryptography is made up of two words "Crypto" and "Graphy" which means hidden writing. These two words "Crypto" and "Graphy" have been take from the Greek language. Cryptography is a process in which the data is transformed into the text which becomes difficult for unintended user to read it. Such a text is also called as the Cipher text.

The recipient at opposite side, decodes or unscramble the message into plain content. Cryptography gives data secrecy, information uprightness, verification and non-repudiation. Secrecy is restricting access or putting limitation on specific sorts of data. Integrity is keeping up and guaranteeing the precision of information being conveyed, i.e., data contains no alteration, cancellation and so on. Verification guarantees the personality of sender and recipient of the data. Non-denial is the capacity to guarantee that the sender or recipient can't prevent the realness from securing their mark on the sending data that they began.

Current age cryptography is synonymous with encryption. Here the first data is known as plain content and scrambled data is known as figure content or the cipher content. The process of cryptography works in three phases or the so called steps:

In the first step the original message generated by the source is encrypted into the non-readable form. Such an unreadable message is also called as the cipher text and the complete process is called as encryption [2].

In the next step, the unreadable message or the cipher text is transferred from the source to the destination through some transmission medium.

In the last step, the recipient of the message receives the cipher text and decode it into the plain text to get the original message. The complete process of encryption and decryption is as shown in figure 1.

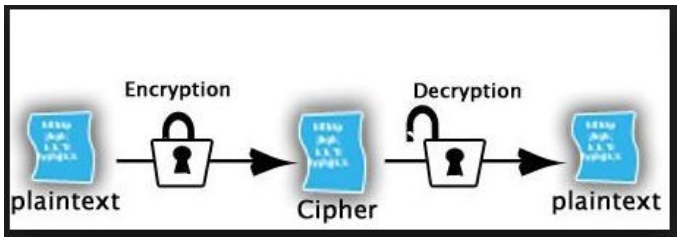

Figure 1. The complete process of Encryption and Decryption

This process of encryption can be performed by more than one ways depending upon the type of key used. One of the way is called symmetric key cryptography and the other is called asymmetric key cryptography.

Symmetric key cryptography: It refers to the cryptography strategies within which the sender and the receiver share an equivalent key. Many encryption algorithms like AES, DES, RC5 etc uses

this methodology of cryptography. Symmetric key cryptography consists of five major components which are the original message, algorithm for encryption, cipher text, key and algorithm for decryption. An algorithm for encryption is used for performing several operations on the plain text using key. The key used is independent of the plain text and is chosen by either sender or the receiver of the message. The receiver uses the decryption algorithm to transform the cipher text back into the plain original message with the help of a secret key. Only the sender and the receiver know this secret key. The process of Symmetric key cryptography is shown in the figure 2.

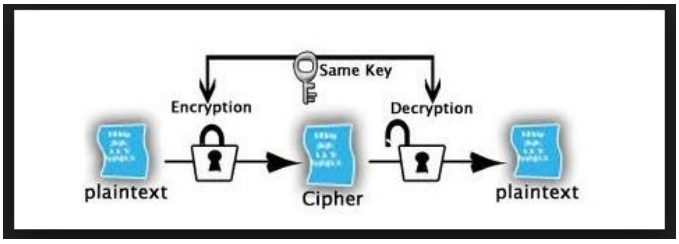

Figure 2. Symmetric Key Cryptography

A noteworthy limitation of symmetric key encryption is that it requires the key to shared by each combine of conveying parties, and furthermore the key itself to be partaken in a secured medium. Any unintended client having the key has a threat of figuring the content.

Asymmetric key cryptography: In this type of encryption technique, two types of keys are used. One of the key is called the private key and the other one is called as public key. The sender transforms the original message into the cipher text with the help of encryption algorithm using public key. The cipher text is then transmitted to the intended user through some transmission media and then the receiver uses the private key to decrypt the message to get the original message [3].

The process of asymmetric key cryptography is as shown in figure 3.

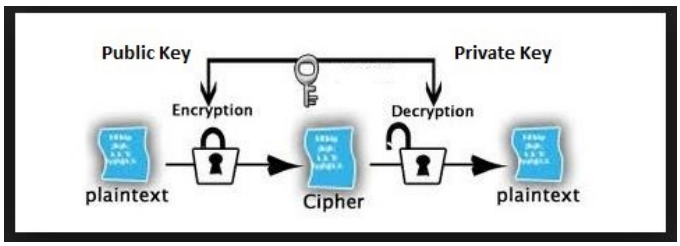

Figure 3. Asymmetric Key Cryptography

Steganography: Steganography is the mechanism of hiding the plain text into images. The word "Steganography" is taken from Greek origin, which means "Hidden writing". At the end of the day, it is the art and exploration of imparting in a way, which shrouds the presence of the correspondence. The objective is to conceal messages inside different innocuous messages in a way that does not enable foe to try to identify that there is a moment message shows. Steganography concentrates more on high security and limit. Indeed, even little changes to stego medium can change its significance. Steganography veils the touchy information in any cover media like pictures, sound, video over the web [4].

Steganography uses following steps in order to hide the secret information:

1. Choice of the cover media in which the information will be covered up.

2. The mystery message or data that is to be veiled in the cover media.

3. A capacity that will be utilized to shroud information in the cover media and its reverse to recover the shrouded information.

4. A discretionary key or the secret word to confirm or to stow away and unhide the information

The cover picked ought to be done deliberately. The cover picked ought to contain adequate excess data which can be utilized to conceal the information,

since steganography works by supplanting the repetitive information with the secret message.
There are three fundamental sorts of steganographic conventions:

1. Unadulterated steganography – it doesn't require the trade of figure, for example, a stego-key however the sender and beneficiary must approach implanting and extraction calculation. The cover for this strategy is chosen to such an extent that it limits the progressions caused by implanting process. These frameworks are definitely not extremely secure as the security relies upon the assumption that no other gathering knows about this secret message.

2. Secret key steganography – these technique employments a key to install the secret message into the cover. The key is just known to sender and the recipient and is known before correspondence. Additionally, the key ought to be traded in a protected medium. The limitation of this approach is that it is helpless to capture attempt.

3. Open key steganography – it utilizes two keys, open key put away out in the open database and is utilized for inserting process and the secret key is known just to correspondence parties what's more, is utilized to remake the first message. The process of steganography is shown in the figure 4.

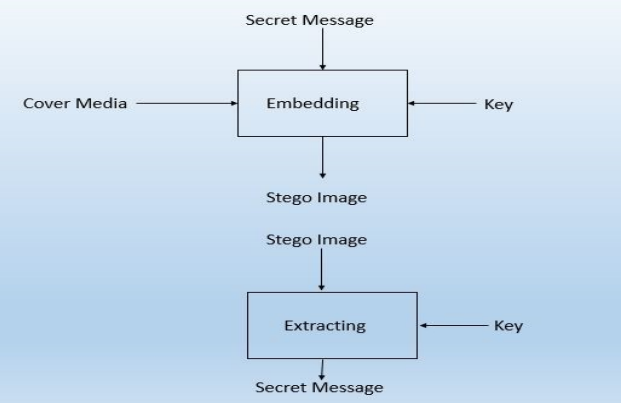

Figure 4. Process of steganography

III. WATERMARKING

A watermark is a conspicuous picture or example that is awed onto paper, which gives proof of its legitimacy. Watermark shows up as different shades of gentility/murkiness when seen in transmitted light. Watermarks are regularly observed as security highlights to banknotes, travel permits, postage stamps and other security papers. Computerized watermarking is an augmentation of this idea in the computerized world.

Today there have been such an extensive amount information over web that it has constrained us to utilize components that can secure responsibility for media. Robbery of advanced data is exceptionally normal, be it pictures, content, sound or on the other hand video. These can be created and dispersed exceptionally effortlessly. Along these lines, it turns out to be imperative to discover who the proprietor of the archive. Advanced watermarking gives an answer for longstanding issues confronted with copyright of advanced information. Advanced watermark is a sort of marker clandestinely inserted to any computerized information, for example, sound or picture information. It can later be removed or identified to make declaration about information. This data can be data about creator, copyright or a picture itself. The computerized watermark stays in place under transmission/change, enabling us to secure our possession rights in computerized shape. Advanced watermarks are just detectable under certain conditions, i.e. in the wake of utilizing some calculation, and indistinct whenever else. On the off chance that a computerized watermark misshapes the transporter motion in a way that it progresses toward becoming distinguishable, it is of no utilization.

A watermarking framework's essential objective is to guarantee robustness, i.e, it ought to be difficult to evacuate the watermark without altering the first information. Computerized watermarking is an

inactive assurance device. It just denotes the information, however does not corrupt it nor controls access to information.

IV. COMPARISON OF DIFFERENT DATA HIDING TECHNIQUES

A. Steganography vs. Cryptography

Steganography signifies "cover expressing" while cryptography signifies "secret stating". Steganography is regularly mistaken for cryptography in any case, there is considerable distinction among two. The previous utilizations a cover to conceal the data and send it to the system. It is troublesome for any unintended client to decide if there is any secret data inserted or not. The critical trademark with steganography is that the cover ought to be picked with enough excess data so that even in the wake of installing the message, it isn't simple to recognize for the message in the wake of taking a look at the message. Though, cryptography includes scrambling the message with the end goal that it is possible that it winds up disjointed or the first significance of the message is altogether changed [5].

Steganography does not adjust the structure of the mystery message while, cryptography adjusts the structure of the secret message. Previous keeps the disclosure of the presence of the correspondence while last keeps unapproved client from finding the substance of a correspondence.

B. Watermarking with Steganography

To ensure the realness of the report, watermarking can be connected to it. This watermarked archive can be inserted in cover picture utilizing a stego-key and transmitted over the correspondence medium. At the beneficiary end, the data can be to begin with decoded utilizing the turnaround method and afterward it. can be approved for its genuineness utilizing the watermarking. This consolidated approach will fulfill every one of the four objectives of information concealing: security, limit, power and detectable quality [6].

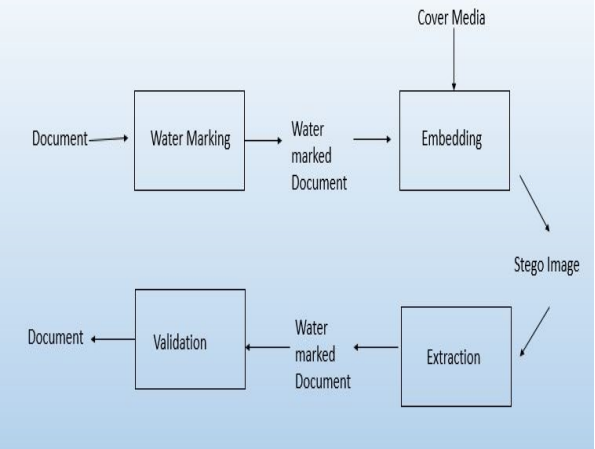

Figure 5. Watermarking with Steganography

C. Cryptography with Steganography

Both the methods can be joined to give one more level of security. The message can be first scrambled utilizing cryptography to a figure content. This figure message at that point can be implanted in a cover media utilizing steganography. This joined approach will fulfill the three objectives of information concealing: security, capacity, robustness [7].

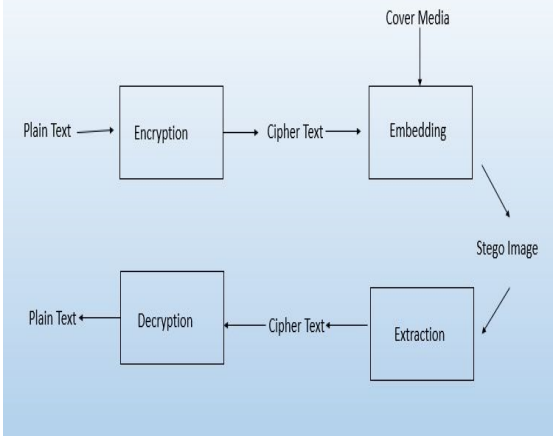

Figure 6. Cryptography with Steganography

V. CONCLUSION

In this paper, we have attempted to give a survey of existing information masking procedures, their favourable circumstances and limitations. This paper likewise explains why information hiding is picking up significance nowadays and the objectives that

must be accomplished of any information concealing method. Also, we have attempted to state how the fundamental objectives of information hiding can be accomplished by consolidating at least one procedures of information hiding.

VI. REFERENCES

[1] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM systems journal, 35(3.4), 313-336.

[2] Boneh, D., & Franklin, M. (2001, August). Identity-based encryption from the Weil pairing. In Annual international cryptology conference (pp. 213-229). Springer, Berlin, Heidelberg.

[3] Aziz, B., & Nourdine, E. (2008, April). A recent survey on key management schemes in manet. In Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on (pp. 1-6). IEEE.

[4] Slavin, K. R. (1999). U.S. Patent No. 5,956,407. Washington, DC: U.S. Patent and Trademark Office.

[5] Nuzzolese, A. G., Pandelli, S., & Ungaro, L. (2005). Steganography vs. Cryptography.

[6] Johnson, N. F., Duric, Z., & Jajodia, S. (2001). Information Hiding: Steganography and Watermarking-Attacks and Countermeasures: Steganography and Watermarking: Attacks and Countermeasures (Vol. 1). Springer Science & Business Media.

[7] Manoj, I. V. S. (2010). Cryptography and steganography. International Journal of Computer Applications (0975–8887), 1(12), 63-68