International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, (2020), pp. 45 - 49

Advance Approach for Securing Secret Information Through the Combination of Reversible Data Hiding and Visual Cryptography Mechanism

Ms.Poonam Mahurkar, Prashant Adakane
PG scholar, Computer Science and Engineering
Professor, Department of Computer Science and Engineering,
G H Raisoni University Amravati.

Abstract

Most of the concepts, security to data and information are provided with either steganography or with the Cryptography concept. This concept has its own drawbacks and limitations that restrict its area of application. The proposed concept has a major objective to overcome the drawbacks that occur in steganography and Cryptography. The concept combines the concept of both these previous techniques and generates a new approach that provides better security from all aspects to sensitive data and information. It is expected to have good results over any other existing techniques that will enhance its acceptability in the future.

Index Terms—*Steganography, cryptography, carrier object, peak signal to noise ratio, mean square error, quantization error, standard deviation, stego object.*

I. INTRODUCTION

Information is a primary source of earning for every industry. Most of the industries process their data to secure their future business. Data science and analysis is entirely base and successful when data is secure on memory storage. Data security is achieved through the concept like cryptography, steganography and digital watermarking. These concepts are called a modern era concept which are good enough to protect data on local as well as hosting server. However, these techniques also have limitations and drawbacks that restrict their application domain. The proposed concept concentrate on the drawbacks and limitations of steganography and visual cryptography and tries to generate a new concept that will use to protect data more efficiently over the local and hosting server. Security concepts are classified according to their working mechanism which is listed in the below figure.The use of these techniques varies from application to application like cryptography is used to protect data stored on memory storage whereas steganography is generally preferable for transmitting data over insecure wireless media.And watermarking is used for copyright protection. Watermarking (example logo) is used to show ownership for a product.

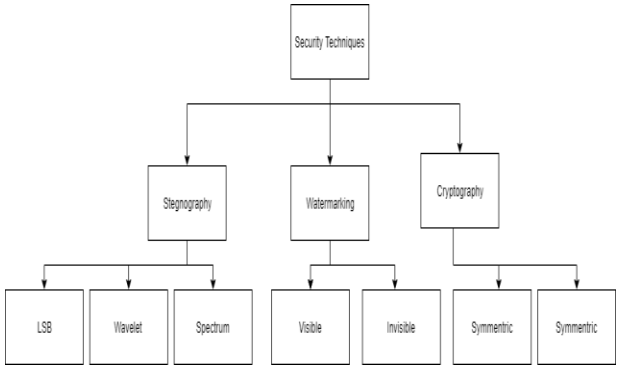

Fig. 1.Classification of security techniques

ISSN: 2233-7857 IJFGCN

A. *Steganography*

It is the art of hiding data behind the carrier object. Career object may be an image, audio, video, and text. Depends on the type of career, steganography is called image, audio, video and text steganography respectively. Data Hiding capacity of these careers varies. Video has maximum Data Hiding capacity due to its two channels i.e frames and audio. Steganography is generally used for transmitting sensitive data on an unsecured wireless network. It completely hides the existence of secret data in a network due to which intruder never gets a clue about the presence of data and hence fails to Intercept or extract data. It's a very powerful tool which comes into exist in 2001 after 9 animal attack on American pentagon Tower.

Steganography takes care not to change the audiovisual perceptual quality of the original career object. Change in career object after hiding data is measured with parameters like peak signal to noise ratio, mean square error, structural content, entropy, average difference, normalized absolute error and other. As original and result and carrier, the object looks exactly similar, it's very difficult for any unknown/unauthorised/ intruder/ ethical hacker to detect the presence of secret data. Quantization error is the measure of the difference between the original sample and the resulting sample is where is from 0 to 255. A sample is made up of 8 bits, a secret data bit can be possible to hide in position from 0 to 7. Hiding secret data from position 0 to 7 increases quantization error due to which most of the programmers prefer to hide data from the least significant bits positions.

B. *Digital Watermarking*

Digital watermarking is used for copyright protection of the product. The best example of digital watermarking is a digital signature, tV channel logo, and others. Watermarking is again classified as visible watermarking and invisible watermarking. Invisible watermarking is also called as steganography. The security of data is not possible with watermarking. It only uses to protect data from unauthorized use. Most of the security applications like email, banking sector prefer watermarking while transmitting it on transmission media. Authenticate receiver confirms the originality of incoming data or messages by analyzing watermarks.

C. *Cryptography*

It is the art of converting readable data into an unreadable format. Cryptography completely hides the meaning of data whereas steganography hides the existence of data. Cryptography can be implemented with algorithms like data Encryption standard, advanced encryption standard, RC2, RSA and other. Algorithms are classified as symmetry and asymmetry cryptography. Sometimes symmetric Cryptography is also called private key cryptography and asymmetry is called as public-key cryptography.

In symmetric-key cryptography, single keys used for data encryption and decryption on the sender and receiver side respectively. Whereas in asymmetric cryptography, two different keys are used for encryption and decryption on sender and receiver side respectively. Symmetric Key Cryptography is considered a powerful tool for securing the meaning of data from unauthorized access. As Cryptography shows the existence of data, it is not a good choice for transmitting sensitive data over an unsecured network especially when transmitting data on the host server without an SSL certificate. Symmetry cryptography is implemented with different sizes of keys like 128, 256, 1024 and it's higher size. More the size of a key, more will be the security to data, but requires more time for encryption and decryption process.

ISSN: 2233-7857 IJFGCN

II. LITERATURE SURVEY

Shraddha S. More; Anagha Mudrale; Sukhada Raut[1] propose a payment system for online shopping based on steganography and visual Cryptography concept. It completely provides security to customer data that prevents misuse of customer data especially account credentials. This method adaptively identifies issue and maintain customer data security efficiently. This method is specially designed for an e-commerce application and focuses on payment security by adding OTP features. This project required work to maintain the features like robustness, accuracy, and others. The application domain of this project is limited to only ecommerce due to the use of only one type of career. Seema Chavan; Y B. Gurav[2] proposes a technique of image steganography in combination with visual cryptography to Secure data on trusted as well as on untrusted channels. The career image has been categorized as unstructured data. the implementation of this concept require big data environment which is interesting work for the future. Data Hiding capacity of this method is limited because it hides only one-bit per sample of career. As the size of carrier increases, the time required for hiding and extracting data also increases. The shares are created from carrier image and secret data is hidden in different shares.

Kunal Hossain; Susovan Jana; Saswati Mukherjee; Ranjan Parekh[3] propose base encoding method that uses discrete cosine transform and flipping technique to create result stego image. ki is generated that is used to authorise receiver during the process of retrieval. These methods can be further extended to determine the security of skin disease images based on their sensitivity. it uses skin disease image as a career object for hiding data. Skin disease image hiding capacity can be further extended based on its sensitivity. The bit error rate of this proposed method is comparatively low with other existing techniques.

Allu Supraja ; Kakelli Anil Kumar[4] shows the visual Cryptography concept is highly important in a trading system while implementing somehow it is Losing what it expected exactly. It uses symmetry key visual cryptography and secret sharing scheme for Data Hiding which avoids attack and also reduces the loss of data during the process of transmission. Signal to noise ratio of their propose method is comparatively high with other existing techniques. The effectiveness of the visual Cryptography algorithm varies is from algorithm to algorithm.

Vijay Kumar Sharma; Pratistha Mathur; Devesh Kumar Srivastava[5] propose a two-way authentication technique that is implemented with visual Cryptography and steganography to protect occurrence of fraud in e-commerce. The main task is to provide security in terms of authentication and identifying unusual activities during data transmission. Propose work is intended only to extract required sensitive data hidden behind career and not to reconstruct the original carrier. This technique is implemented on grayscale and black and white types of images. Numbers of shares are created on the sender side that uses a discrete wavelet transform technique for Data Hiding.

Samaneh Shafee; Boshra Rajaei[6] hide data in Digital Image by using a compressive sensing technique that increases the security of stego image. Status today results mostly on 512 X 512 gray scale size images. The performance of this proposed method is measured with peak signal to noise ratio etc. This the normal traffic technique based on the human visual system. This method is not applicable to colour images due to occurrence of difference between the original and results stego image. changes occur in result career is observable with factor like mean square error, absolute difference, structural content, normalised absolute error etc.

Faisal M. Alawwad; Wadood Abdul; Hatim Behairy; Amr Alasaad[7] proposes the Least Significant Matched Revisited Algorithm(LSBMR) for hiding data. This method is based on the pre-processing of the secret image to reduce the amount of possible bits modification. They hide data randomly in which the

ISSN: 2233-7857 IJFGCN

probability of LSBMR occurrence will maximize and it gives a better signal to noise ratio performance. This technique use secret data of small size. The messages divided into sub-messages which are hidden in two different parts of career object based on least difference. This technique generates additional information that keeps the positions of a hidden secret base. This additional information is used to extract data on the receiver side from stego carrier.

V. Keral Shalini; T. Abirami[8] proposes a method that hides secret Database from the Most Significant Bit position to the least significant bit position. quantization error can be reduced by shifting MSB position two LSB bits. The occurrence of quantization error depends on what position secret bit get hidden. This process requires an additional effort of flipping carrier sample bits.

III. CONCLUSION

An extensive study has been done based on concepts of steganography and visual cryptography. More than 50+ standard quality papers have been referred and the conclusion has taken out listed below

1. Most of the techniques less Data Hiding capacity.
2. Data Hiding capacity where is from least significant bit to most significant bit.
3. Available Visual cryptography are working on grayscale images or on RGB colour model images.
4. There is a need to have a concept that combines visual Cryptography and steganography to invent a new approach that overcomes limitations and drawbacks of existing techniques.
5. The number of shares generated in the various techniques of visual cryptography is limited which should be required to further extend for increasing a Data Hiding capacity.
6. Data Hiding capacity of different careers is highly dependent on their size. It means every technique have limited Data Hiding capacity.
7. Present era need to have infinite Data Hiding capacity irrespective of the size of carrier object.
8. If combination of visual cryptography, steganography and data compression is used, that will make possible to hide more data greater than the size of career.

REFERENCES

[1] Shraddha S. More ; Anagha Mudrale ; Sukhada Raut, "Secure Transaction System using Collective Approach of Steganography and Visual Cryptography" 2018 International Conference on Smart City and Emerging Technology (ICSCET)

[2] Seema Chavan ; Y B. Gurav,"Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing for Image Processing" 2018 International Conference on Inventive Research in Computing Applications (ICIRCA)

[3] Kunal Hossain ;Susovan Jana ; Saswati Mukherjee ;Ranjan Parekh", Secured transmission of sensitive images of skin diseases using steganography and cryptography",2017 IEEE Calcutta Conference (CALCON)

[4] Allu Supraja ; Kakelli Anil Kumar," Analysis on Hybrid Approach for (K, N) Secret Sharing in Visual Cryptography",2019 International Conference on Data Science and Communication (IconDSC)

ISSN: 2233-7857 IJFGCN

[5] Viiay Kumar Sharma ; Pratistha Mathur ; Devesh Kumar Srivastava,"Secure Electronic Fund Transfer Model based on Two level Authentication", 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)

[6] Mamta ; Mayank Deep Khare ; Chandra Shekhar Yadav," A secure steganography algorithm using compressive sensing based on HVS feature", 2017 Seventh International Conference on Emerging Security Technologies (EST)

[7] Faisal M. Alawwad ; Wadood Abdul ; Hatim Behairy ; Amr Alasaad,"An improved LSBMR steganography based on message interleaving approach", 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)

[8] V. Keral Shalini ; T. Abirami,"High secure digital image steganography for secrete communication",2017 Third International Conference on Science Technology Engineering Management (ICONSTEM)

[9] Branislav Madoš ; Anton Balaz ; Norbert Adám ; Ján Hurtuk,"Information Hiding into OBJ Format File Using Vector Steganography Techniques",2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI)

[10] Anjum Ara ; Deepa Gianchandani,"A Hybrid Approach Based 3d Image Steganography Instead of 2d Image for Exchange Information",2018 3rd International Conference on Communication and Electronics Systems (ICCES)

[11] Arup Kumar Chattonadhvav ; Debalina Ghosh ; Ram Sekher Pati ; Amitava Nag ; Sanchita Ghosh,"Visual Cryptography: Review and Analysis of Existing Methods",2018 Global Wireless Summit (GWS)

[12] Xiang Li ; Guangtao Zhai ; Jia Wang ; Ke Gu,"Portable information security display system via Spatial PsychoVisual Modulation",2017 IEEE Visual Communications and Image Processing (VCIP)

[13] Siva Janakiraman ; Vinoth Raj ; K. Thenmozhi ; Rengarajan Amirtharajan,"Optimized Lightweight Image Steganography on Embedded Device via LUT Approach",2019 International Conference on Computer Communication and Informatics (ICCCI)

ISSN: 2233-7857 IJFGCN