A Brief Survey on Data Hiding Methods

Vivek Jaladi[1], Baswaraj Gadgay[2]
[1]*Department of ECE, Lingaraj Appa Engineering College, Bidar, Karnataka, India*
[2] *Department of ECE, UBDT College of Engineering, Davangere, Karnataka, India*

***Abstract*- This paper gives the description of the Data Hiding methods with Reversible and Tunable Scrambling Embedding (RTSE) method to scramble an image and include the confidential information in it by using row and column rotation. To embed the data the two methods are used; irreversible and reversible. The predicted locations are vacated to embed information while degrading the image. The control over the perceptual quality is controlled in embedded-scrambled image. The prediction errors are stored in a predetermined precision which will use the structure size information. The stored prediction error precision can be adjusted for controlling the perceptual information quality of reconstructed image.**

***Index Terms*- Tunable scrambling, data hiding, data mining, reconstructed image.**

I. INTRODUCTION

Modern day's technology provides the full-fledged infrastructure for this generation users. In today's scenario most of the people can easily capture, store, and modify the data with the help of affordable digital device. In day-to-day life maximum peoples are highly depend on internet for sending text messages, sharing pictures, online job application, on-line shopping, online matrimonial services, exchange e-mails, on-line chatting, video conferencing/chat, storing the data in the cloud, sharing the pictures/video through social network websites, etc. These all on-line activities are done with the hope of safety of their information. To facilitate these services online one should take the responsibility of safety of the information. To give support to this cause the hiding of the data comes into a picture, where one can use the safety measures to ensures the safety.

The hiding of information uses many algorithms such as DES (1999), AES (2001) etc. The protection of highly sensitive data viz., credit card information, passwords and confidential data is very much essential. In such cases there is tremendous need to efficiently administrate and protect the information from being misused by other persons. To avoid this scrambling technology is invented to obscure the perceptual meaning of a multimedia content, protecting the original content from unauthorized viewing. On the other hand, data embedding is proposed to insert external information into the host content.

The information embedded within various components can be varied depending upon the benefits of the application, e.g., visible watermark to authorization of the user, description or hyper-linking to enrich the content. To hide the personal information mainly two techniques were used that is scrambling and reversibility. The scrambling technology makes use of the digital image to embed the information in it and let it to travel over the internet, whereas reversibility means bring back the real information from the scrambled information or else we can say reconstructing the original content.

II. INFORMATION HIDING

The hiding of information is the science and art of providing secrecy of communication (Neil F.Johnson & Jajodia, 2011) has designed a method to achieve hiding of information in two forms viz., encryption and external data insertion (Rad, Wong, & Guo, 2014).

The encryption seal the perceptual informative multimedia content by converting it into an unintelligible form (i.e., resemble white noise) (Van De Ville, Philips, Van De Walle,& Lemahieu, 2004; Karim & Wong, 2014).

A) Scrambling

Scrambling is treated as an alternative method for encryption. Scrambling is designed to overcome some application and developing constraint such as

time, space complexity and format compliance while little bit compromising to robustness. This method is also called lightweight encryption, perceptual encryption, or transparent encryption from the literature.

The scrambling method is achieved using permutation (changing of position) and substitution (replacing with other value). The design of scrambling suits for the requirement of application which has lower security and application which requires processing a large amount of data. Lastly, scrambling is also said as quality degradation.

B) Scalability

The term scalability refers to the Image quality degradation and the ability to offer more carrier capacity when necessary. The external data insertion is aiming to achieve high output image quality hence the achievable embedding capacity is limited. The unified information hiding is aiming to gain external data insertion and scrambling at the same time.

III. REVERSIBLE DATA EMBEDDING

Reversible data embedding falls under three main categories those are (a) histogram shifting (b) expansion based (c) compress-and-append. With the use of peak and empty bins from the image histogram external data information can be embedded. In other words it embeds the information in cover media by shifting the histogram of the image. This technique yields higher data hiding capacity with low distortion. Also histogram shifting technique prevents overflow and underflow problem. Overflow is the condition that the gray value exceeds above 255. Underflow is the condition that the gray value falls below 0. For expansion based technique data embedding is done using the difference between two adjacent pixel values then embed data in the prediction errors. compress its residuals (i.e., quantization errors) to vacate space for data embedding. Then, the compressed residuals and payload are appended to the host signal using the generalized LSB modification method. This method also provides scalability in terms of distortion and payload. However, the aforementioned Reversible data embedding methods aim to embed data while maintaining high image quality.

The reversible data embedding, its is called lossless data embedding, embeds invisible data (payload) into a digital image in a fashion of reverse. The initial requirement, the quality degradation on the image after data embedding is low. An intriguing feature of reversible data embedding is the reversibility, that is, one can remove the embedded data to restore the original image. From the information hiding point of view, reversible data embedding hides some information in a digital image in such a way that an authorized party could decode the hidden information and also restore the image to its original, pristine state. The motivation of reversible data embedding is distortion-free data embedding. Though imperceptible, embedding some data will inevitably change the original content. Even a very slight change in pixel values may not be desirable, especially in sensitive imagery, such as military data and medical data. In such a scenario, every bit of information is important. Any change will affect the intelligence of the image, and the access to the original, raw data is always required.

IV. TUNABLE SCRAMBLING EMBEDDING

The decoding process is also called tunable scrambling, the operations in must be first reversed (i.e., decoding) to enable correct image reconstruction and data extraction. This flow of process prevents the unauthorized party to recover the original image and the embedded data without the valid keys. Using the management scenario the unauthorized viewer needs the valid key to restore the original pixel values because they are substituted by other values, i.e., modified .On the other hand, the secretary can only access to the administrative metadata from column-based decoding process without being able to view the original image. Finally, a manager with the highest authority level has access to both the original image and the embedded confidential data after the row-based decoding operation.

V. WATERMARKING REVERSIBLE

The advent of the Internet and the wide availability of computers and printers make digital data exchange and transmission a simple task. A digital watermark is an invisible signature embedded inside an image to

show authenticity and ownership. An effective digital watermark should be perceptually invisible to prevent obstruction of the original image. It should be statistically invisible to prevent detection, and it should also be robust to many image manipulations, such as filtering, additive noise, and compression. Digital Watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including copy prevention and control. Digital watermarking has been proposed as a new, alternative method to enforce the intellectual property rights and protect digital media from tampering. It involves a process of embedding into a host signal a perceptually transparent digital signature, carrying a message about the Signature is called the digital watermark. The digital watermark contains data that can be used in various applications, including digital rights management, broadcast monitoring and tamper proofing. Although perceptually transparent, the existence of the watermark is indicated when watermarked media is passed through an appropriate watermark detector. Digital watermarking has become an active and important area of research, and development and commercialization of watermarking techniques is being deemed essential to help address some of the challenges faced by the rapid Proliferation of digital watermarking technique of an image.

VI. EXTRACTION OF IMAGES

In machine learning, pattern recognition and in image processing, image extraction starts from an initial set of measured data and builds derived values (features) intended to be informative, non-redundant, facilitating the subsequent learning and generalization steps, in some cases leading to better human interpretations. Image extraction is related to dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be redundant (e.g. the same measurement in both feet and meters, or the repetitiveness of images presented as pixels), then it can be transformed into a reduced set of features (also named features vector). This process is called image extraction. The extracted images are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data. After embedding process the image is extracted from the cover image

V. CONCLUSION

In this paper discussed briefly about the scrambling of images, reversible data embedding, tunable scrambling embedding method, reversible watermarking and extraction of images from scrambled images also. In next work embed to scramble and then extraction process will be discussed.

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, (2010), “Digital Image Steganography: Survey and Analysis of Current Methods”, Elsevier signal processing, Vol. 90, pp. 727-752.

[2] Jun Tian, “Reversible Data Embedding Using a Difference Expansion”, IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, august 2003.

[3] Ali Al-Ataby and Fawzi Al-Naima,(2010), “ A Modified High Capacity Image Steganography Technique Based on Wavelet Transform”, The International Arab Journal of Information Technology, Vol. 7, No. 4, pp 357-363.

[4] Bret Dunba r, (2002), “A detailed look at stegonagraphic Techniques and their use in an Open – Systems Environment”, SANS Institute.

[5] Shruti M. Rakhunde, Archana A. Nikose, “New Approach for Reversible Data Hiding Using Visual Cryptography”, IEEE International Conference on Computational Intelligence and Communication Networks 2014, Print ISBN: 978-1-4799-6928-9, Pages 846 – 855

[6] Chang C.C, Lin C.C and Chen Y.H,(2008), “ Reversible Data Embedding Scheme using Differences Between Original and Predicted Pixel values” , IET Information Security, Vol. 2

[7] Chin-Chen Chang, Wei-Liang Tai, and Chia-Chen Lin, (2006), “A Reversible Data Hiding Scheme Based on Side Match Vector Quantization”, IEEE Transaction on Circuits and Systems for Video Technology, Vol.16, No. 10, pp 1301-1308.

[8] Coltuc D and Tremeau A,(2005), " Simple Reversible Watermarking Schemes ", Proc. of SPIE, Security, Steganography, Watermarking of Multimedia Contents, Vol. 5681, pp. 561–568.

[9] Dalel Bouslimi, Gouenou Coatrieux, Michel Cozic and Christian Roux, (2012), "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images", IEEE Transactions on Information Technology in Biomedicine, Vol. 16, No.5, pp. 891- 899.

[10] Shruti M. Rakhunde, Archana A. Nikose, "A Novel and Improved Technique for Reversible Data Hiding using Visual Cryptography", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 6, June 2014, ISSN (Online) : 2278-1021, ISSN (Print) : 2319-5940

[11] Neil F. Johnson, Z. D., & Jajodia, S. (2001). Information hiding steganography and watermarking attacks and counter measures. Norwell, MA, USA: Kluwer Academic Publishers.

[12] Rad, R., Wong, K., & Guo, J.-M. (2014, April). A unified data embedding and scrambling method. IEEE Transactions on Image Processing, 23(4), 1463 - 1475.

[13] Van De Ville, D., Philips, W., Van De Walle, R., & Lemahieu, I. (2004). Image scrambling without bandwidth expansion. IEEE Transactions on Circuits and Systems for Video Technology, 14(6), 892- 897.