International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.297-306
http://dx.doi.org/10.14257/ijsia.2014.8.4.27

Survey on Reversible Data Hiding Techniques

[1]M. Manju and [2]Dr.V.Kavitha

[1]Assistant Professor, Department of CSE,
Jayamatha Engineering College,
Aralvaimozhi, India
Email Id: mmanju_gem@yahoo.co.in
[2]Associate Professor, Department of CSE,
University College of Engineering, Nagercoil, Konam, India.
kavinayav@gmail.com

Abstract

With the fast improvement of multimedia technologies and the rising attractiveness of the internet, information or data hiding methods have become more and more extensively applied to achieve authentication. Data hiding methods are ways of embedding additional messages into host signals by modifying their original contents without introducing perceptual changes. The main aim of the paper is to present a survey on traditional data hiding techniques which are mainly based on reducing the embedding distortions.

Keywords: Data embedding, Reversible Watermarking, Data Integrity, Embedding Capacity

1. Introduction

Security is considered to be the most critical factor in many applications. The main issues of such security based systems are integrity, privacy, authenticity and non-repudiation and these four issues are to be carefully addressed. The three goals of security namely confidentiality, integrity and availability can be threatened by security attacks. Figure 1 relates the taxonomy of attack types to security goals. Threat is a potential for violation of security which exists when there is a circumstance that could cause harm. Threat is a possible danger that might exploit vulnerability. Confidentiality refers to the protection of transmitted data from unauthorized disclosure. Integrity refers to the assurance that the data received are exactly the same as that of an authorized sender. Availability refers to the availability of the system resources to the authorized entity on demand. Snooping and traffic analysis monitors the network activity thereby producing miscellaneous effect. Modification means that a portion of the message is being altered or reordered to produce unauthorized effect. Masquerade takes place when on entity pretends to be another entity. Replay attack is a form of threat to integrity and it is defined as a type of network attack in which a valid data transmission is maliciously repeated or delayed. It involves the passive capture of the data unit and its subsequent retransmission produces unauthorized effect. Denial of Service prevents the normal communication facilities by disrupting the entire network.

ISSN: 1738-9976 IJSIA

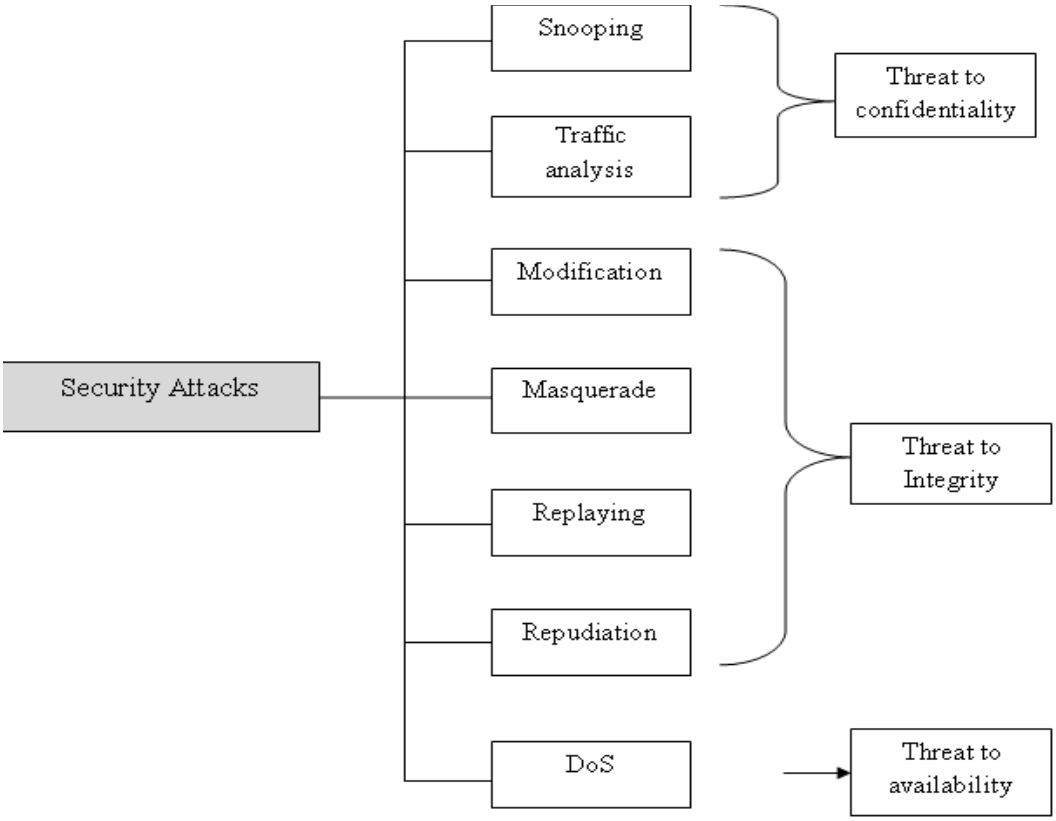


Figure 1. Taxonomy of Attacks

Data hiding is a technique which embeds data into digital media to communicate secret messages by slightly varying the content of the media, so that the embedding data is unnoticeable. Many anticipated techniques are data hiding are non-reversible which means the embedded media are distorted and cannot be restored. If the embedded media can be recovered through a specifically considered algorithm, then the data hiding technique is termed as reversible. When a digital image is used to embed data, the image that is used to carry data is called as the cover image and the image with the embedded data is called as the stego image. Images in certain applications like images in military, medical etc., allows no distortions. In these areas of applications, data hiding techniques gives a clarification to the deformation problem since the original cover image can be entirely recovered.

This paper is organized as follows: Part 2 deals with the various reversible data hiding techniques, Part 3 deals with the comparison of those techniques and finally a brief conclusion section is given which summarizes the paper.

2. Reversible Data Hiding (RDH) Techniques

Data hiding is a group of methods that are used to insert a secure data in a shot media with small deterioration in the host. Reversible data hiding inserts information bits by modifying the host data and enable lossless reconstruction of the original host data after extracting the embedded information. The various reversible data hiding techniques are discussed in detail below:

2.1 Data Hiding Scheme with Edge Prediction and Difference Expansion (Method -1)

This method is a novel multiple-base lossless scheme based on JPEG-LS pixel value prediction mechanism to decrease the distortion caused by the hiding of secret data. It employs multiple-base notational system to increase the payload of the image.

2.1.1 Embedding Procedure

In this scheme, the embedding procedure consists of three steps, including the pixel value prediction for reducing the distortion, the capacity estimation to achieve a higher payload and finally the difference expansion that completes the embedding procedure as shown in Figure 2.

In the prediction phase, the pixels in the top-most row and the left-most column of a cover image are preserved without any secret data hidden in them. The embedding capacity of a pixel is determined by the variance of its neighbor pixels. The embedding capacity varies from pixel to pixel because the pixels in smoother areas are responsible for embedding more secret data with high accuracy and less prediction error. Then the secret message is transformed into various bases by using a multiple-base notational system. In the embedding phase, by having the predictive pixel value and its base, embedding is done by using the following steps:

i) The top-most and the left-most column are not used for hiding data; the stego pixel value P^1_{ij} equals $P_{ij.}$

ii) The secret data s_{dk} is read and it is converted into a decimal value.

iii) Compute the difference value d_{ij} between the original pixel value P_{ij} and the predictive value P^1_{ij} as follows:

$$d_{ij} = P_{ij} - P^1_{ij} \quad (1)$$

The remainder value r_{ij} of the secret data is to be embedded with the base by using the equation given below:

$$r_{ij} = s_{dk} \bmod P_{ij} \quad (2)$$

iv) According to the base b_{ij}, the original difference value d_{ij} can be expanded b_{ij} times. The new difference d^1_{ij} is obtained as follows:

$$d^1_{ij} = d_{ij} \times b_{ij} + r_{ij}$$

v) Obtain the new stego image P^{11}_{ij} as follows:

$$P^{11}_{ij} = P^1_{ij} + d^1_{ij}$$

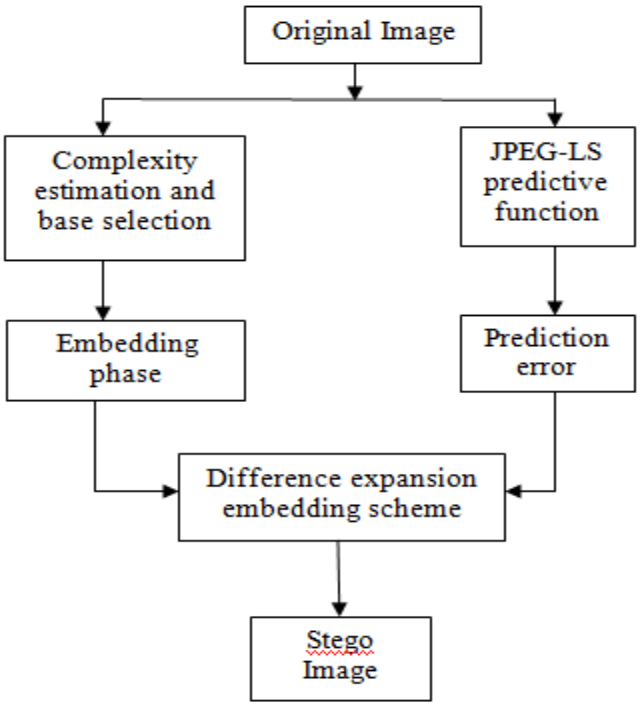


Figure 2. Embedding Procedure

2.1.2. Data Extraction Procedure

The steps to extract the secret data from the stego image and to recover the original pixel values of the cover image are explained as below:

i) Since the top-most and the left-most column pixels do not carry any secret data, these pixels can be easily recovered by $P_{ij.} = P^{11}_{ij}$.

ii) For each stego pixel P^{11}_{ij} with its three adjacent pixels, the predictive value P^{11}_{ij} can be obtained as follows:

$$X1 = \begin{cases} \min(a, b), & \text{if } c >= \max(a,b) \\ \max(a, b), & \text{if } c <= \min(a, b) \\ a + b + c, & \text{otherwise} \end{cases} \quad (3)$$

iii) Then the variance value is calculated and base is also determined.

iv) The new difference d^1_{ij} is calculated as $d^1_{ij} = P^{11}_{ij} - P^1_{ij}$

v) Extract the secret message by extracting the remainder the original difference value $d_{ij.}$

vi) Finally, the original cover pixel value P_{ij} is recovered as $P_{ij} = P^1_{ij} - d_{ij.}$

Advantages:

- Embedding payload is increased.
- Fewer distortions
- Capable of hiding more secret data.

Disadvantage:

- High complexity.

2.2. Data Hiding Scheme Using Orthogonal Projection and Prediction Error Modification (Method -2)

The data hiding scheme is based on histogram shifting and prediction error modification. Orthogonal Projection Technique (OPT) is used for the optimal determination of the weights involved in a linear predictor [1]. According to OPT, the value of the current pixel is predicted by a weighted sum of three of its previously visited neighbors.

2.2.1. Embedding Procedure

Let I be the cover image with size M x M. The steps involved in the embedding process are explained below:

i) The weights of the cover image is optimally determined sing the OPT method.
ii) The histogram of the prediction error is constructed and the best shifting direction d is obtained.
iii) Obtain the peak p of the error histogram. Let N+ and N- be the number of prediction errors that is larger than p and smaller than p respectively.
iv) Scan the prediction errors E.
   a. if the scanned error is equal to p, then a secret bit s extracted from the message S is then embedded into the prediction error by using E' = E + sd
   b. If the scanned error is not equal to p, the prediction errors have to be shifted according to the shifting direction.
      i. If d=1, those prediction errors larger than the peak value have to be added by one.
      ii. If d=-1, the prediction error less than peak value has to be subtracted by one.
v) The stego image is then constructed by calculating I'=E' + I

2.2.2. Data Extraction Procedure

To extract the embedded data, the stego image is scanned using the same order as in the embedding phase to obtain the modified prediction errors. According to the values of the modified prediction errors, the secret data can be extracted and the original prediction errors can be restored. Finally the original cover image can be recovered by using the original prediction errors.

Advantages:

- High prediction accuracy.
- High embedding capacity.

Disadvantage:

- Recovered image quality is not good.

2.3. Low Distortion Transform for Reversible Watermarking (Method 3)

The basic principle of this method is to reduce the distortion introduced by the watermarking by embedding not only in to the current pixel but also in to its prediction context [5]. For performing the algorithm, consider the linear predictor called the fourth predictor of JPEG. The proposed embedding scheme covers a 2 x 2 block. Let n, w and nw be the north, west and north-west neighbors of pixel x respectively as shown in Table 1.

Table 1. Pixel and Its Neighbors

nw	n
w	x

2.3.1 Embedding Procedure:

The embedding procedure ensures minimization of the square error introduced by the watermarking**.** The steps involved in the embedding process are explained below:

i) Pixel x is estimated as $\hat{x}$ = n + w – nw.
ii) The difference is calculated as p = x - $\hat{x}$
iii) The prediction error $P_b = p + b$ where 'b' is the bit to be embedded.
iv) Split $P_b$as evenly as possible in to four parts as d_x, d_n, $d_w$and d_{nw}. These values are calculated as follows:

$$d_x = \left\lfloor \frac{P_b}{4} \right\rfloor \qquad d_w = \left\lfloor \frac{Pb+1}{4} \right\rfloor \tag{4}$$

$$d_{nw} = \left\lfloor \frac{Pb+2}{4} \right\rfloor \qquad d_n = \left\lfloor \frac{Pb+3}{4} \right\rfloor \tag{5}$$

Here $\lfloor a \rfloor$ rounds 'a' towards minus infinity.

v) With this distributions, the new set of pixels become X, N,W and NW and are calculated as follows:

$$X = x + d_x \qquad W = w + d_w \tag{6}$$

$$NW = nw + d_{nw} \qquad N = n + d_n \tag{7}$$

2.3.2. Data Extraction Procedure

The steps involved in the recovering process are explained below:

i) Pixel X is estimated as $\hat{X}$ = N +W – NW.
ii) The difference is calculated as P =X - $\hat{X}$ = 2p + b
iii) Embedded data bit 'b' forms the LSB of X - $\hat{X}$
iv) Recover p as $p = \frac{X-\hat{X}-b}{2}$
v) Compute d_x, d_n, $d_w$and d_{nw} as follows:

$$d_x = \left\lfloor \frac{P_b}{4} \right\rfloor \qquad d_w = \left\lfloor \frac{Pb+1}{4} \right\rfloor \tag{8}$$

$$d_{nw} = \left\lfloor \frac{Pb+2}{4} \right\rfloor \qquad d_n = \left\lfloor \frac{Pb+3}{4} \right\rfloor \tag{9}$$

Here $\lfloor a \rfloor$ rounds 'a' towards minus infinity.

vi) Finally the original pixels are recovered as follows:

$$x = X - d_x \qquad w = W + d_w \tag{10}$$

$$nw = NW - d_{nw} \qquad n = N + d_n \tag{11}$$

Advantages:

- Easy processing.
- High embedding capacity.
- Better recovered image quality.
- Very low distortion.

3. Comparison and Discussion

To evaluate the performance of the above explained three methods, eight test images are taken and the Peak-Signal-to-Noise values are noted along with embedding capacity and the payload. The PSNR is a measure of the peak error between two images in decibels. It is computed as shown in Equation (12).

$$PSNR = 10 \log_{10} \left[\frac{R^2}{MSE}\right] \quad (12)$$

Here, R = 255.

Thus PSNR compares how far the original image and the reconstructed image are equal. A higher value of the PSNR represents the better quality of the reconstructed image. MSE represents the cumulative squared error between the reconstructed and the original image. The low value of MSE represents the lower error in the reconstruction of the image. The MSE value is computed as given by Equation (13). In Equation (13), M and N are the number of rows and columns in the input images.

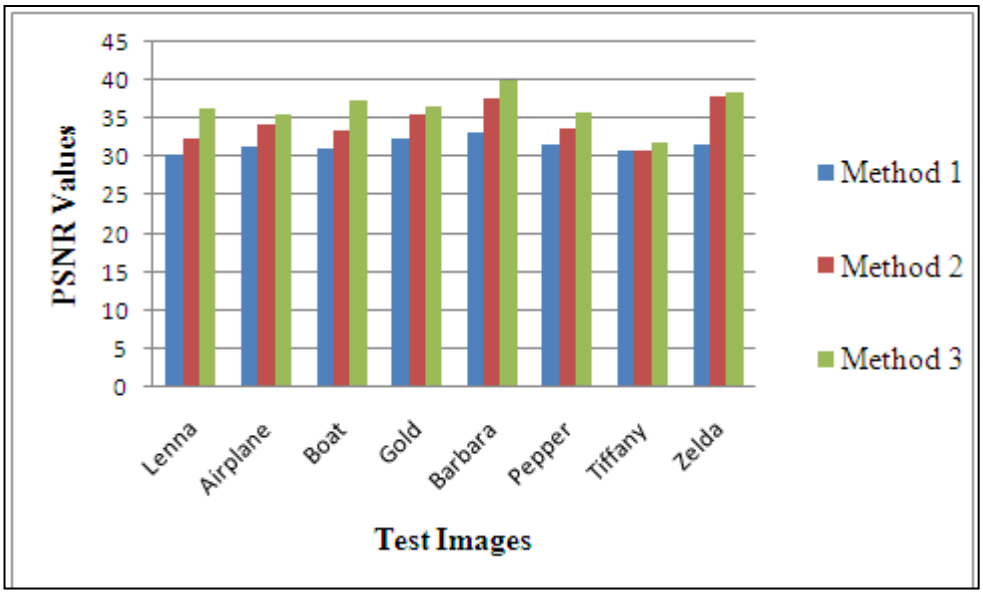
$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)^2]}{M * N} \quad (13)$$

The embedding capacity is defined as the number of bits per pixel that are modified to embed its payload in to the carrier signal. The secret message is generated by a pseudo random number generator with identical probabilities for bit 1 and for bit values 0. Table 2 summarizes the PSNR values and embedding capacity for all the three methods.

Table 2. Performance Measures for Method 1

Test Image (512 x 512)	Method 1		Method 2		Method 3	
	PSNR (dB)	Embedding Capacity (bpp)	PSNR (dB)	Embedding Capacity (bpp)	PSNR (dB)	Embedding Capacity (bpp)
Lenna	30.30	1.22	32.45	1.54	36.45	1.65
Airplane	31.35	1.57	34.37	1.67	35.56	1.87
Boat	31.01	1.17	33.40	1.22	37.40	1.23
Gold	32.33	0.83	35.65	0.87	36.65	0.99
Barbara	33.29	0.70	37.79	0.89	39.96	0.91
Pepper	31.54	1.23	33.66	1.23	35.78	1.29
Tiffany	30.83	1.34	30.98	1.57	31.99	1.67
Zelda	31.68	1.31	37.89	1.56	38.33	1.66

Graph 1 and Graph 2 shows the comparative evaluation for the three methods based on PSNR values and embedding capacity.



Graph 1. Comparative Evaluation based on PSNR Values

Graph 2. Comparative Evaluation based on Embedding Capacity Values

It is observed from the above graphs that the low distortion transform based watermarking technique produces better PSNR values and higher embedding capacity than the other data hiding techniques.

4. Conclusion

In this paper, different reversible digital watermarking techniques have been studied along with their performance. It is observed that the low distortion transform based watermarking method gives better results in terms of PSNR values and embedding capacity values.

References

[1] W. Hong, T. S. Chen, Y. P. Chang and C. W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification", Signal Processing, vol. 90, **(2008)**, pp. 35-46.
[2] X. Zhang, "Reversible data hiding in Encrypted image", IEEE Signal Processing Letters, vol. 18, no. 4, **(2011)**.
[3] D. Coltuc and J. M. Chassery, "Very fast watermarking by reversible contrast mapping", IEEE Signal Processing Letter, vol. 14, no. 4, **(2007)**, pp. 255-258.
[4] D. Coltuc, "Low distortion transform for reversible watermarking", IEEE Transactions on Image Processing, vol. 21, no. 1, **(2012).**
[5] L. Kamstra and H. J. A. M. Heijmans, "Reversible data embedding in to images using wavelet techniques and sorting", IEEE Trans. Image Process, vol. 14, no. 12, **(2005)**, pp. 2082-2090.
[6] L. Luo, Z. Chen, X. Zeng and Z. Xiong, "Reversible image watermarking using interpolation technique", IEEE Transactions on Information Forensics Security, vol. 5, no. 1, **(2010)**, pp. 187-19.
[7] Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding", IEEE Trans. Circuits Syst. Video Technology, vol. 16, no. 3, **(2006)**, pp. 354-364.
[8] V. Sachnev, H. J. Kim, J. Nam, S. Suresh and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction", IEEE Trans. Circuits Systems Video Technology, vol. 19, no. 7, **(2009)**, pp. 989-999.
[9] J. Tian, "Reversible data embedding using a difference expansion", IEEE Transaction Circuits Systems Video Technology, vol. 13, no. 8, **(2003)**, pp. 890-896.

Authors

M. Manju, she is a Ph. D student doing her research in Computer Science and Engineering, Anna University, Tirunelveli under the guidance of Dr. V. Kavitha. She obtained her B.E degree in Electrical and Electronics Engineering in 1998 from MS University and ME degree in Computer Science and Engineering in 2000 from Madurai Kamaraj University. Presently she is working as Asst. Prof in the Department of CSE at Jayamatha Engineering College. Her research interests are Network Security, Image Processing and Multimedia Compression. She has published many papers in National and International Conferences. She is a life time member of ISTE.

V. Kavitha, she obtained her B.E degree in Computer Science and Engineering in 1996 from MS University and ME degree in Computer Science and Engineering in 2000 from Madurai Kamaraj University. She is the University Rank Holder in UG and Gold Medalist in PG. She received PhD degree in computer science and Engineering from Anna University Chennai in 2009. Right from 1996 she is in the Department of Computer Science & Engineering under various designations. Presently she is working as Associate Professor in the Department of CSE at University College of Engineering, Konam, Nagercoil. Currently, under her guidance ten Research Scholars are pursuing Ph. D as full time and part time. Her research interests are Wireless networks Mobile Computing, Network Security, Wireless Sensor Networks, Image Processing, Cloud Computing .She has published many papers in national and International journal in areas such as Network security, Mobile Computing, wireless network security, and Cloud Computing. She is a life time member of ISTE.