Reversible Data Hiding

Yun Q. Shi

Department of Electrical and Computer Engineering,
New Jersey Institute of Technology,
Newark, NJ 07102, USA
shi@njit.edu

Abstract. Reversible data hiding, in which the stago-media can be reversed to the original cover media exactly, has attracted increasing interests from the data hiding community. In this study, the existing reversible data hiding algorithms, including some newest schemes, have been classified into three categories: 1) Those developed for fragile authentication; 2) Those developed for achieving high data embedding capacity; 3) Those developed for semi-fragile authentication. In each category, some prominent representatives are selected. The principles, merits, drawbacks and applications of these algorithms are analyzed and addressed.

1 Introduction

Digital watermarking, often referred to as data hiding, has recently been proposed as a promising technique for information assurance. Owing to data hiding, however, some permanent distortion may occur and hence the original cover medium may not be able to be reversed exactly even after the hidden data have been extracted out. Following the classification of data compression algorithms, this type of data hiding algorithms can be referred to as *lossy* data hiding. It can be shown that most of the data hiding algorithms reported in the literature are lossy. Here, let us examine three major classes of data hiding algorithm. With the most popularly utilized spread-spectrum watermarking techniques, either in DCT domain [1] or block 8x8 DCT domain [2], *round-off* error and/or *truncation* error may take place during data embedding. As a result, there is no way to reverse the stago-media back to the original without distortion. For the least significant bit-plane (LSB) embedding methods, the bits in the LSB are substituted by the data to be embedded and the bit-replacement is *not memorized*. Consequently, the LSB method is not reversible. With the third group of frequently used watermarking techniques, called quantization index modulation (QIM) [3], *quantization* error renders lossy data hiding.

In applications, such as in law enforcement, medical image systems, it is desired to be bale to reverse the stego-media back to the original cover media for legal consideration. In remote sensing and military imaging, high accuracy is required. In some scientific research, experimental data are expensive to be achieved. Under these circumstances, the reversibility of the original media is desired. The data hiding schemes satisfying this requirement can be referred to as *lossless*. The terms of *reversible*, or *invertible* also used frequently. We choose to use reversible in this paper.

I.J. Cox et al. (Eds.): IWDW 2004, LNCS 3304, pp. 1 – 12, 2005.

In Section 2, we classify the reversible data hiding techniques that have appeared in the literature over the past several years into three different categories. In each category, the most prominent representatives are selected and the principles, merits, drawbacks and applications of these algorithms are analyzed in Sections 3, 4, and 5, respectively. Conclusions are drawn in Section 6.

2 Classification of Reversible Data Hiding Algorithms

The following list contains, to our knowledge, most of reversible data hiding algorithms published in the literature. The list is not expected to be completed as the research in this area continues to make vigorous progress. These algorithms can be classified into three categories: 1st, those for fragile authentication, 2nd, those for high embedding capacity, and 3rd, those for semi-fragile authentication. Among each category, one or two prominent algorithms are selected as representative. Their fundamental idea and scheme to achieve reversibility, and their performance are discussed in the following sections.

1.	Barton's U.S. Patent 5,646,997 (97)	(1st)
2.	Honsinger et al.'s US Patent 6,278,791 B1 (01)	(1st)
3.	Fridrich et al.'s method (SPIE01)	(1st)
4.	de Vleeschouwer et al.'s method (MMSP01)	(3rd)
5.	Goljan et al.'s method (IHW01)	(2nd)
6.	Xuan et al.'s method (MMSP02)	(2nd)
7.	Ni et al.'s method (ISCAS03)	(2nd)
8.	Celik et al.'s method (ICIP02)	(2nd)
9.	Tian's method (CSVT03)	(2nd)
10.	Yang et al.'s method (SPIE04)	(2nd)
11.	Thodi & Rodríguez's method (SWSIAI04)	(2nd)
12.	Ni et al.'s method (ICME04)	(3rd)
13.	Zou et al.'s method (MMSP04)	(3rd)
14.	Xuan et al.'s method (MMSP04)	(2nd)
15.	Xuan et al.'s method (IWDW04)	(2nd)

3 Those for Fragile Authentication

The first several reversible data hiding algorithms developed at the early stage belong to this category. Since fragile authentication does not need much data to be embedded in a cover medium, the embedding capacity in this category is not large, normally between 1k to 2k bits. For a typical 512×512 gray scale image, this capacity is equivalent to a data hiding rate from 0.0038 bits per pixel (bpp) to 0.0076 bpp.

In this category, we choose Honsinger et al.'s patent in 2001 [5] as its representative. It describes in detail a reversible data hiding technique used for fragile authentication. Their method is carried out in the image spatial domain by using modulo-256 addition. In the embedding, $Iw = (I + W)$ mod 256, where Iw denotes the marked image, I an original image, W is the payload derived from the hash function of the original image. In the authentication side, the payload W can be extracted from the marked image by subtracting the payload from the marked image, thus reversibly recovering the original image. By using modulo-256 addition, the issue of over/underflow is avoided. Here, by over/underflow, it is meant that grayscale values either exceeding its upper bound (*overflow*) or its lower bound (*underflow*). For instance, for an 8-bit gray image, its gray scale ranges from 0 to 255. The overflow refers to grayscale exceeds 255, while the underflow refers to below 0. It is clear that either case will destroy reversibility. Therefore this issue is often a critical issue in reversible data hiding. Using modulo-256 addition can avoid over/underflow on the one hand. On the other hand, however, the stego-image may suffer from the salt-and-pepper noise during possible grayscale flipping over between 0 and 255 in either direction due to the operation of modulo-256 addition. The effect caused by salt-and-pepper noise will become clear when we discuss an algorithm also using modulo-256 addition in the third category.

4 Those for High Data Embedding Capacity

All the reversible data hiding techniques in the first category aim at fragile authentication, instead of hiding large amount data. As a result, the amount of hidden data is rather limited and may not be suitable for applications such as covert communications and medical data systems. Hence, Goljan et al. [10] presented a first reversible data hiding technique, referred to as R-S scheme, which is suitable for the purpose of having high data embedding capacity. Later, a difference expansion scheme was developed by Tian [15], which has greatly advanced the performance of reversible data hiding in terms of data embedding capacity versus PSNR of marked images with respect to original images. Recently, some integer wavelet transform based reversible data hiding schemes have been developed by Xuan et al. [16,17], which have demonstrated superior performance over that reported in [15]. These representative schemes are presented in this section.

4.1 R-S Scheme

The mechanism of this scheme is described as follows. The pixels in an image are grouped into non-overlapped blocks, each consisting of a number of adjacent pixels. For instance, it could be a horizontal block consisting of four consecutive pixels. A discrimination function that can capture the smoothness of the groups is established to classify the blocks into three different categories, Regular, Singular and Unusable. An invertible operation F can be applied to groups. That is, it can map a block from one category to another as $F(R)=S$, $F(S)=R$, and $F(U)=U$. It is invertible since applying it to a block twice produces the original block. This invertible operation is hence called *flipping F*. An example of the invertible operation F can be the permutation between 0 and 1, 2 and 3, 3 and 4, and so on. This is equivalent to flipping the least significant bit (LSB). Another example is the permutation between 0 and 2, 1 and 3, 4 and 6, and so on, i.e., flipping the second LSB. Apparently, the *strength* of the latter flipping is stronger than the former. The principle to achieve reversible data embedding lies in that there is a bias between the number of regular blocks and that of singular blocks for most of images. This is equivalent to say that there is a redundancy and some space can be created by lossless compression. Together with some proper bookkeeping scheme, one can achieve reversibility.

The proposed algorithm first scan a cover image block-by-block, resulting in a so-called RS-vector formed by representing, say, an R-block by binary 1 and an S-block by binary 0 with the U groups simply skipped. Then the algorithm losslessly compresses this RS-vector − as an overhead for bookkeeping usage in reconstruction of the original image late. By assigning binary 1 and 0 to R and S blocks, respectively, one bit can be embedded into each R or S block. If the bit to-be-embedded does match the type of a block under consideration, the flipping operation F is applied to the block to obtain a match. The actual embedded data consist of the overhead and the watermark signal (pure payload). In data extraction, the algorithm scans the marked image in the same manner as in the data embedding. From the resultant RS-vector, the embedded data can be extracted. The overhead portion will be used to reconstruct the original image, while the remaining portion is the payload.

While it is novel and successful in reversible data hiding with a large embedding capacity, the amount of data that can be hidden by this technique is still not large enough for some applications such as covert communications. From what is reported in [10], the estimated embedding capacity ranges from 0.022 bpp to 0.17 bpp when the embedding strength is six and the PSNR of the marked image versus the original image is about 36.06 dB. Note that the embedding strength six is rather high and there are some block artifacts in the marked image generated with this embedding strength. On the one hand, this embedding capacity is much higher than that in the first category discussed in the previous subsection. On the other hand, however, it may be not high enough for some applications. This limited embedding capacity is expected because each block can at most embed one bit, U blocks cannot accommodate data, and the overhead is necessary for reconstruction of the original image. Another problem with this method is that when the embedding strength increases, the embedding capacity will increase, at the same time the visual quality will drop. Often, block artifacts will take place at this circumstance, thus causing visual quality of marked image to decrease.

4.2 Difference Expansion Scheme

Tian presented a promising high capacity reversible data embedding algorithm in [15]. In the algorithm, two techniques are employed, i.e., difference expansion and generalized least significant bit embedding, to achieve a very high embedding capacity, while keep the distortion low. The main idea of this technique is described below. For a pair of pixel values x and y , the algorithm first computes the integer average l

and difference h of x and y, where $h = x - y$. Then h is shifted to the left-hand size by one bit and the to-be-embedded bit b is appended into the LSB. This is equivalent to $h' = 2 \times h + b$, where h' denotes the expanded difference, which explains the term of Difference Expansion. Finally the new x and y, denoted by x' and y', respectively, are calculated based on the new difference values h' and the original integer average value l. In this way, the stego-image is obtained. To avoid over/underflow, the algorithm only embeds data into the pixel pairs that shall not lead to over/underflow. Therefore, a two-dimensional binary bookkeeping image is losslessly compressed and embedded as overhead.

Note that the above-mentioned relationship between the pair of integers x and y versus the pair of integers l and h is implemented in the following manner.

$$\begin{aligned} l &= \lfloor 0.5 \times (x+y) \rfloor & \qquad x &= l + \lfloor 0.5 \times (h+1) \rfloor \\ h &= x - y & \qquad y &= l - \lfloor 0.5 \times h \rfloor \end{aligned} \tag{1}$$

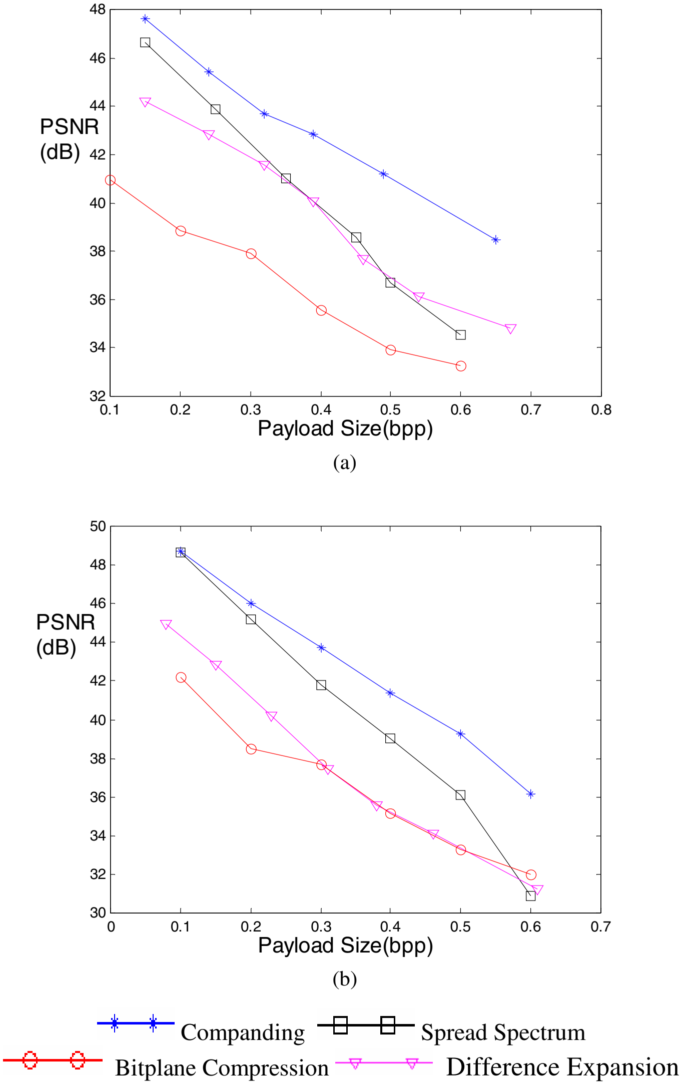
where the floor operation is utilized. According to integer Haar transform, it is reversible between these two integer pairs. Apparently, the reversible transformation between integers avoids round-off error. This together with the bookkeeping data mentioned above guaranteed reversibility.

It has been reported in [15] that the embedding capacity achieved by the difference expansion method is much higher than that achieved by [10]. This does not come with surprise since intuitively each pair of pixels can possibly embed one bit, while only each block of pixels can possibly embed one bit.

4.3 Integer Wavelet Transform Based Schemes

Xuan et al. proposed three high capacity reversible data hiding algorithms based on integer wavelet transform (IWT) [11, 16, 18]. These three algorithms have three features in common. The first is that they are all implemented in the IWT domain. Consideration is as follows. IWT as a WT is known to be able to decorrelate signal well in the transformation domain. Its feature consists with that of our human vision system (HVS). WT can be implemented efficiently by using lifting scheme. IWT can further ensure the reversible forward wavelet transform and inverse wavelet transform. For these reasons, IWT have been used in JPEG2000 for lossless compression. It is shown in Xuan et al.'s algorithms that IWT plays an important role in reversible data hiding. The second feature is that these algorithms all contain a preprocessing stage, histogram modification, in order to prevent overflow and underflow. That is, an efficient scheme has been developed to shrink the histogram towards the center, leaving two ends empty. Consequently, the perturbation caused by modification of selected IWT coefficients will not cause overflow and underflow. For reversibility, the histogram modification parameters need to be embedded as overhead. Because of the efficiency of the modification scheme [12], the overhead is not heavy. The third feature is that all of three algorithms embed data in IWT coefficients of high frequency subbands. This is because the modification of coefficients in these subbands will be imperceptible if the magnitude of the modification is not large.

The first algorithm [11, 12] losslessly compresses some selected middle bit-planes of IWT coefficients in high frequency subbands to create space to hide data. Since the bias between binary 1 and 0 in the bit-planes of IWT high frequency coefficients becomes much larger than that in the spatial domain, this method achieves rather higher embedding capacity than [7], that is the counterpart of this algorithm in spatial domain.



(a)

(b)

Fig. 1. Comparison results on Lena (left) and Barbara (right) images

The second algorithm [16] uses spread spectrum method to hide data in IWT coefficients in high frequency subbands. Pseudo bits are used to indicate those coefficients that are not selected for data embedding, thus saving overhead data. As a result, this method is more efficient than the bit-plane compression scheme, described above.

The third method [18] uses companding technique for data embedding, which was inspired by [17]. Based on the study of statistical distribution of IWT coefficients in high frequency subbands, a piecewise linear companding function is designed.

The performance of these three algorithms, applied to two typical test images: Lena and Baboon, are shown in Figure 1 in terms of data embedding capacity versus PSNR. It is clear that the IWT-based companding algorithm performs best. This can be explained from an investigation on the amount of magnitude that the selected IWT high frequency coefficients have been changed and how many coefficients are required to embed one bit during the data embedding by these three algorithms. It can be shown that the companding algorithm causes the least amount of changes in the selected IWT coefficients among the three algorithms, followed by the spread-spectrum algorithm, while both the spread-spectrum and companding algorithms can embed almost one bit into one IWT high frequency coefficient. Note that both IWT-based companding and spread-spectrum algorithms have outperformed the difference expansion algorithm, discussed above in this section.

It is noticed that more and more advanced algorithms in this category are being and to be developed. One recent example is shown in [24]

5 Those for Semi-fragile Authentication

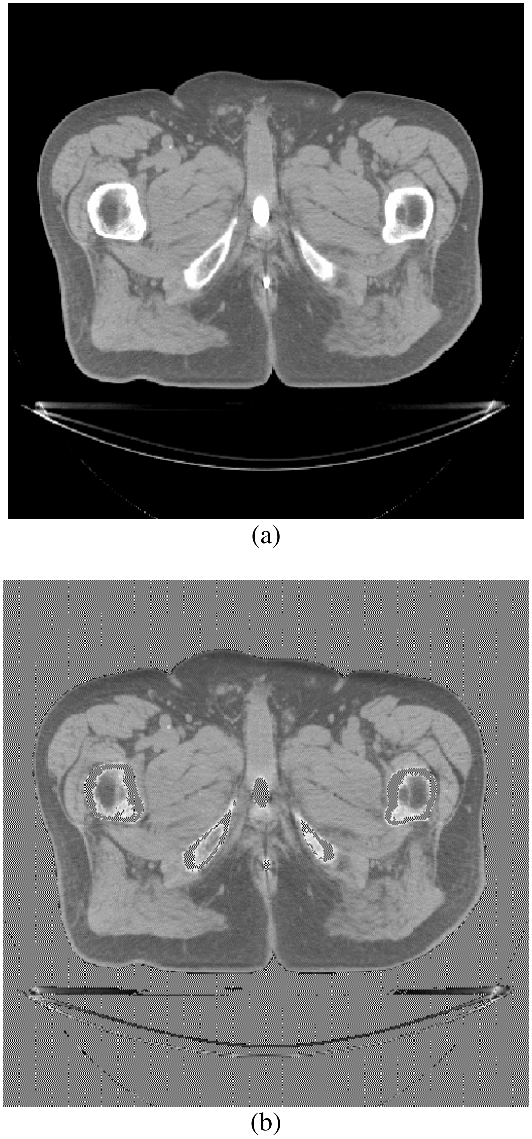
For multimedia, content-based authentication makes more sense than representation-based authentication. This is because the former, often called semi-fragile authentication, allows some incidental modification, say, compression within a reasonable extent, while the latter, called fragile authentication, does not allow any alteration occurred to stego-media, including compression. For instance, when an image goes through JPEG compression with a high quality factor, the content of this image is considered unchanged from the common sense. Hence, it makes sense to claim this compressed image as authentic. For the purpose of semi-fragile authentication, we need reversible data hiding algorithms that are robust to compression, maybe called semi-fragile reversible data hiding or robust reversible data hiding. This can be further illustrated by the following scenario. In a newly proposed JPEG2000 image authentication framework [19], both fragile and semi-fragile authentications are included. Within the semi-fragile authentication, both cases of lossy and lossless compressions are considered. In this framework, some features corresponding to an image below a pre-specified compression ratio are first identified. By “corresponding” it is meant that these features will remain as long as the compression applied to the image is below this pre-specified compression ratio. The digital signature of these features is reversibly embedded into the image. Then in the verification stage, if the marked image has not been changed at all, the hidden signature can be extracted and the original image can be recovered. The matching between the extracted signature and the signature generated from the reconstructed (*left-over*) image renders the image authentic. If the marked image has been compressed with a compression ratio below the pre-specified one, the original image cannot be recovered due to the lossy compression applied, but the hidden signature can still be recovered without error and verify the compressed image as authentic. Obviously, if the marked image goes through a compression with the compression ratio higher than the pre-specified ratio will render the image un-authentic. Any malicious attack will render the attacked image non-authentic owing to the resultant dismatch between the extracted signature and the signature generated from the received image after the hidden data extraction. A robust lossless data hiding algorithm is indeed necessary for this framework. In general, robust lossless data hiding can be utilized in lossy environment.

5.1 Patchwork-Based Scheme Using Modulo-256 Addition

De Vleeschouwer et al. [20] proposed a reversible data hiding algorithm based on patchwork theory [21], which has certain robustness against JPEG lossy compression. This is the only existing robust reversible data hiding algorithm against JPEG compression. In this algorithm, each hidden bit is associated with a group of pixels, e.g., a block in an image. Each group is pseudo-randomly divided into two subsets of equal number of pixels, let's call them Zones A and B. The histogram of each zone is mapped into a circle in the following way. That is, each point on the circle is indexed by the corresponding luminance, and the number of pixels assuming the luminance will be the weight of the point. One can then determine the *mass* center of each zone. It is observed that in the most cases the vectors pointing from the circle center to the mass center of Zones A and B are *close* (almost equal) to each other because the pixels of Zone A and Zone B are highly correlated for most of images. Considering a group, rotating these two vectors in two opposite directions by a small quantity, say, rotating the vector of Zone A counter-clockwise and rotating the vector of Zone B clockwise allows for embedding binary 1, while rotating the vector of Zone A clockwise, and the vector of Zone B counter-clockwise embeds a binary 0. As to the pixel values, rotation of the vector corresponds to a shift in luminance. In data extraction, the angles of the mass center vectors of both Zone A and Zone B versus the horizontal direction are first calculated, and the difference between these two angles are then determined. A positive difference represents a binary 1, while the negative a binary 0.

One major element of this algorithm is that that it is based on the patchwork theory. That is, within each zone, the mass center vector's orientation is determined by all the pixels within this zone. Consequently, the algorithm is robust to image compression to certain extent. Another major element of this algorithm lies in that it uses modulo-256 addition to avoid overflow and underflow, thus achieving reversibility. Consequently, however, as pointed out in Section 3, this algorithm will suffer from the salt-and-pepper noise. One example from our extensive investigation is presented in Figures 2. In the stego-medical image, the severe salt-and-pepper noise is clear. The PSNR of stego-image versus the original image is below 10 dB when 476 information bits are embedded into this 512x512 image. Not only for medical image, the salt-and-pepper noise may be severe for color images as well. We have applied this algorithm to eight JPEG2000 test color images. There are four among the eight images that suffer from severe salt-and-pepper noise, while the other four some less severe salt-and-pepper noise. The PSNR can be as low as less than 20 dB when severe noise exists when 1412 information bits are embedded into a color image of 1536x1920x24.

From the above investigation, it can be concluded that all reversible data hiding algorithms based on modulo-256 addition to avoid overflow and underflow, say, in [5] and [20] cannot be applied to many real applications, and hence should be avoided.



(a)

(b)

Fig. 2. (a) Original medical image, (b) Stego-image with severe salt-and-pepper noise. 746 information bits are embedded into the image of 512x512 with a PSNR of the stego-image versus the original image lower than 10 dB

5.2 Patchwork-Based Scheme Without Using Modulo-256 Addition

Realizing that modulo-256 addition, though can prevent overflow and underflow and hence achieve reversibility, causes stego-images suffer from annoying salt-and-pepper noise, Ni et al. have developed a new reversible data hiding scheme that does not use modulo-256 addition [22]. It is based on the patchwork theory to achieve the semi-fragility in data hiding. Specifically, it identifies a statistical quantity within a block of pixels which is robust to minor alteration of pixel values within the block, and manipulates it to embed a bit into the block. Together with additional measures including error correction coding and permutation, it thus achieves semi-fragility (or in other words, robustness). The reversibility is gained by using a novel strategy in data embedding. That is, it classifies a block of pixels into four different categories according to the distribution of pixel grayscale values within the block. For blocks in different categories, a different embedding strategy is used.

This novel semi-fragile reversible data hiding algorithm has achieved superior performance over the semi-fragile reversible data hiding algorithm using modulo-256 addition. It was reported in [22] that their method has been applied to all of eight medical test images, including that shown in Figure 2 (a), to embed the same amount of data (746 information bits in the images of 512x512). In all of eight stego-images, there is no salt-and-pepper noise at all. The PSNR of all of eight medical images are above 40 dB, indicating a substantial improvement in the quality of stego-images.

Another novel semi-fragile reversible data hiding algorithm with the similar idea as in [22] implemented in integer wavelet transform domain has been reported in [23]. Some special measures have been taken to avoid overflow and underflow.

These two algorithms have been utilized in a unified framework of authentication of JPEG2000 images. The framework has been included into the Security Part of JPEG2000 (known as JPSEC), CD 1.0 in April 2004 [19].

6 Conclusion

This article presents an investigation on the development of the existing reversible data hiding techniques. These techniques are classified into three different categories. The principles, merits and drawbacks of each category are discussed. It is shown that the reversible data hiding opens a new door to link two groups of data: cover media data and to-be-embedded data. This will find wide applications in information assurance such as authentication, secure medical data system, and intellectual property protection to name a few.

Acknowledgement

The work has been supported in part by the Digital Data Embedding Technologies group of the Air Force Research Laboratory, Rome Research Site, Information Directorate, Rome NY, under contract F30602-03-1-0264. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation there on. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of Air Force Research Laboratory, or the U.S. Government. It has also been supported in part by New Jersey Commission of Science and Technology via New Jersey Center of Wireless Network and Internet Security (NJWINS).

References

1. I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," in *IEEE Trans. on Image Processing*, vol. 6. No. 12, pp. 1673-1687, Dec. 1997.
2. J. Huang and Y. Q. Shi, "An adaptive image watermarking scheme based on visual masking," *Electronics Letters*, 34 (8), pp. 748-750, 1998.
3. B. Chen, G. W. Wornell, "Quantization index modulation: a class of provably good methods for digital watermarking and information embedding," *IEEE Transaction on Information Theory,* vol. 47, no. 4, pp. 1423-1443, May 2001.
4. J. M. Barton, "Method and apparatus for embedding authentication information within digital data," U.S. Patent 5,646,997, 1997.
5. C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless recovery of an original image containing embedded data," US Patent: 6,278,791, 2001.
6. R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Upper Saddle River, NJ: Prentice Hall, 2001.
7. J. Fridrich, M. Goljan and R. Du, "Invertible authentication," *Proc. SPIE, Security and Watermarking of Multimedia Contents*, pp. 197-208, San Jose, CA, January 2001.
8. J. Fridrich, M. Goljan and R. Du, "Invertible Authentication Watermark for JPEG Images," *Proc. IEEE ITCC 2001,* Las Vegas, Nevada, pp. 223-27, April 2001.
9. J. Fridrich, Rui Du, Lossless "Authentication of MPEG-2 Video," *Proc. IEEE ICIP 2002*, Rochester, NY.
10. M. Goljan, J. Fridrich, and R. Du, "Distortion-free data embedding," *Proceedings of 4th Information Hiding Workshop*, pp. 27-41, Pittsburgh, PA, April 2001.
11. G. Xuan, J. Zhu, J. Chen, Y. Q. Shi, Z. Ni, W. Su "Distortionless Data Hiding Based on Integer Wavelet Transform," *IEE journal, ELECTRONICS LETTERS,* Volume 38, No 25, pp.1646-1648, Dec.2002.
12. G. Xuan, Y. Q. Shi, Z. C. Ni, J. Chen, C. Yang, Y. Zhen, J. Zhen, "High capacity lossless data hiding based on integer wavelet transform," *IEEE International Symposium on Circuits and Systems*, Vancouver, Canada, May 2004.
13. M. Celik, G. Sharma, A.M. Tekalp, E. Saber, "Reversible data hiding," in *Proceedings of the International Conference on Image Processing 2002*, Rochester, NY, September 2002.
14. Z. Ni, Y. Q. Shi, N. Ansari and W. Su, "Reversible data hiding," *IEEE International Symposium on Circuits and Systems,* Bangkok, Thailand, May 2003.
15. J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transaction on Circuits and Systems for Video Technology*, Vol. 13, No. 8, August 2003.
16. G. Xuan, Y. Q. Shi, Z. Ni, "Lossless data hiding using integer wavelet transform and spread spectrum," *IEEE International Workshop on Multimedia Signal Processing*, Siena, Italy, September 2004.

17. B. Yang, M. Schmucker, W. Funk, C. Busch, S. Sun, "Integer DCT-based reversible watermarking for images using companding technique," *Proceedings of SPIE Vol. #5306*, January 2004.
18. G. Xuan, Y. Q. Shi, Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," *Proc. IWDW04*, Korea, October 2004.
19. Z. Zhang, Q. Sun, X. Lin, Y. Q. Shi and Z. Ni, "A unified authentication framework for JPEG2000 images," *IEEE International Conference and Expo*, Taipei, Taiwan, June 2004.
20. C. De Vleeschouwer, J. F. Delaigle and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Tran. Multimedia,* vol. 5, pp. 97-105, March 2003.
21. W. Bender, D. Gruhl, N. Mprimoto and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, pp. 313-336, vol. 35, Nos. 3&4, 1996.
22. Z. Ni, Y. Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust lossless data hiding," *IEEE International Conference and Expo*, Taipei, Taiwan, June 2004.
23. D. Zou, Y. Q. Shi, Z. Ni, "lossless data hiding," *IEEE International Workshop on Multimedia Signal Processing*, Siena, Italy, September 2004.
24. M. Thodi and J. J. Rodríguez, "Reversible watermarking by prediction-error expansion," *Proceedings of 6th IEEE Southwest Symposium on Image Analysis and Interpretation*, pp. 21-25, Lake Tahoe, CA,USA, March 28-30, 2004.