4th WSEAS International Conference on ELECTRONICS, CONTROL and SIGNAL PROCESSING, Miami, Florida, USA, 17-19 November, 2005 (pp.70-74)

A High Capacity Image Steganographic System

YUK YING CHUNG
School of Information Technologies
University of Sydney
NSW 2006, Sydney
AUSTRALIA

Abstract: - With the development of mobile communication and internet technologies digital media can be transmitted conveniently over the network. In this process the algorithms used to protect secret messages during transmission become an important issue. This paper presents a new high capacity image steganograpic model based on Discrete Cosine Transform (DCT), Vector Quantisation (VQ) and a Pseudo Random Number Generator (PRNG). The proposed new system can embed more information than traditional algorithms without compression. The recovered hiding image has high Peak Signal to Noise Ratio (PSNR) value and good visual quality. This system is robust in terms of both JPEG compression and other signal processing attacks.

Key-Words: - DCT, VQ, PRNG, digital watermarking

1 Introduction

Steganography is the ancient art of conveying messages in a secret way such that only the receiver knows the existence of the message. The techniques of steganography can be classified into linguistic steganography and technical steganography. The former consists of linguistic or language forms of hidden writing. The disadvantage is that users must equip themselves with good knowledge of linguistics.

The encrypted message using classic cryptography only cannot pass the checkpoint on the network. Steganography provides another layer of protection to the secret message, which will be embedded in another media in such a way that the transmitted data will be meaningful to everyone. Steganography conceals the existence of the secret messages when compared with cryptography techniques which attempt to conceal the content of messages.

In this paper, the signature image was first applied to a Pseudo Random Number Generator (PRNG) to determine the position of the embedding bits and frequencies. Then the signature image was quantised using vector quantisation with the Linde-Buzo-Grey (LBG)[1] algorithm in order to hide larger amounts of watermark data. Binary bits of watermark were embedded directly into the Least Significant Bit (LSB) [2][3] of DCT coefficients in an image. Using the duplication of copies of the watermark provides further robustness against the attacks of signal processing techniques. To extract the watermark the LSB can be taken out and the VQ encoded watermark data can then be decoded by the VQ decoder using source codebook. This method is self-extractable.

Section 2 provides an introduction to the Pseudo Random Number Generator (PRNG). Section 3 explains the implementation of the high capacity image steganographic system. Section 4 and 5 provide the experimental result and conclusion respectively.

2 Introduction to Pseudo Random Number Generator

In order to increase the protection of the secret information, we use the Pseudo Random Number Generator (PRNG) [6] to determine the position of the embedding bits and frequencies. We also use PRNG to shuffle the embedding watermark image before being embedded into the host image. The PRNG can generate uniform and non-uniform distributions and has been used to deal with security concerns. We chose the secret key K as the seed of PRNG in order to generate the random position for the embedding bits and frequency. In the watermark decoding process we use the same secret key K to generate the same random position. We can retrieve the watermark by reconstruction of the retrieved bits to original order.

The PRNG [6] algorithm is based on linear recurrence:

$$X_{k+n} := X_{k+m} \oplus \left(X_k^u \mid X_{k+1}^l\right)A, (k = 0,1,.....)$$

n is the degree of recurrence, r is an integer defined as $0 \le r \le w\text{-}1$, an integer m defined as $1 \le m \le n$, and a constant w by w matrix A with entities either 0 or 1.

The implementation of the above equation is described as follows:

Let x[0 : n – 1] be an array of n unsigned integers of word size, *i* be an integer variable, and *u*, *ll*, a be unsigned constant integers of word size.

(1) $u \leftarrow \underbrace{0\cdots0}_{w-r}\underbrace{1\cdots1}_{r}$;
(Bit mask for upper w – r bits)

$ll \leftarrow \underbrace{0\cdots0}_{w-r}\underbrace{1\cdots1}_{r}$;
(Bit mask for lower w – r bits)

$a \leftarrow a_{w-1}a_{w-2}\cdots a_1a_0$;
(the last row of the matrix A)

(2) i ← 0
x[0], x[1], …, x[n – 1] ←
"any non-zero initial values"

(3) y ← (x[i] AND u) OR (x[(i+1) mod n] AND *ll*);
(computing $\left(X_i^u \mid X_{i+1}^l\right)$)

(4) x[i] ← x[(i + m) mod n] XOR (y >>1)
XOR 0 if the least significant bit of y = 0
XOR 1 if the least significant bit of y = 1
(multiplying A)

(5) (calculate x[i]T)
y ← x [i]
y ← y XOR (y >> u)
(shift right y by u bits and add to y)
y ← y XOR ((y << s) AND b)
y ← y XOR ((y << t) AND c)
y ← y XOR (y >> l)
output y

(6) i ← (i+1) mod n

(7) Go to Step 2

3 Implementation of the high capacity image steganographic system

Our new high capacity image steganographic system is based on a Discrete Cosine Transform (DCT) watermarking model using Vector Quantization (VQ) and Pseudo Random Number Generator (PRNG) to compress the hiding image before being embedded into the cover image.

The steps of the encoding process are as follows:

1. The watermark image is put into a one dimensional array W.
2. Using the secret key K as the seed of PRNG a sequence of permutation positions is generated for all the pixels inside the W so that all the pixels may find a new and distinct position, resulting a new array W',
3. The host image is divided and applied with DCT and Zig-zag transformation,
4. Using the PRNG and the secret key K the random frequency and random LSB position is generated to embed the watermark, and
5. The watermark is embedded and applied with inverse Zig-zag and IDCT transform.

The steps of the decoding process are as follows:

1. The watermarked image is divided and applied with DCT and Zig-zag transformation,
2. Using the same secret key K with PRNG, the same random number will be generated again. Therefore, the previous embedding watermark position can be determined by reproducing the frequency and LSB position, and
3. The embedded bits are retrieved from the watermark to form a one-dimension array W'. Then the secret key K and PRNG are used to reproduce the permutation positions and rearrange the pixels to W, which is the retrieved watermark. For example, the first pixel in the original watermark that is denoted as W[0], will be rearranged to the permutation position to 57, W'[57] = W[0]. When decoding the PRNG, the permutation position 57 is reproduced at position 0. Therefore, W[0] = W'[57].

4 Results and discussion

The Peak Signal to Noise Ratios (PSNR) is used to measure the distortion of a watermarked image.

$$PSNR = 10\log_{10}[\frac{255^2}{\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{i,j} - x_{i,j}')^2}]$$

Where $x_{i,j}$ and x_{ij}' denote the pixels of the original and reproduced images, and the images are the size *M x N*.

Figures 1 and 2 show the image quality of the watermarked host images and retrieved watermark images without use of VQ and PRNG. Figures 3 and 4 show the image quality of the watermarked host images and retrieved watermark images with VQ and PRNG.

The results show that the low frequency level produces a good quality watermark but degrades the quality of the host image. The low frequency level holds the majority of information and when attacks are targeted on the surface of the image low frequency bits get modified significantly. Hence the quality of the embedded watermark is reduced dramatically.

The high frequency level produces less degradation of the host image with an average quality of watermark being retrieved. The high frequency level contains the least amount of information, so when distortion is applied, the quality of embedded watermark degrades significantly. It is concluded that the mid frequency level gives the best quality of the host image and watermark, and at the same time provide resistance to certain attack.

The embedding frequency position test showed that the best frequency range for embedding a watermark is the mid frequency, positioned at the 20^{th} , 21^{th} and 22^{th} in the Zig-zag array, and the best LSB position to embed the watermark in each frequency range is the 5^{th} LSB. The results have also demonstrated that when the frequency level used to embed the watermark information decreased from high to low, the image quality of the retrieved watermark increased and image quality of the host image decreased. This is due to the fact that the low frequency range contains more useful information which has higher visibility in the human vision than the high frequency range. Furthermore the LSB positions have also affected the quality of the retrieved watermark image and the host image. The higher LSB position increases the retrieved watermark quality, and at the same time it decreases the host image quality. The explanation is that the high LSB modifies the embedded binary number dramatically. Hence the quality of the host image degrades. The quality of the retrieved watermark image using random generated LSB position provides similar quality, and it provides more security than the traditional scheme.

In order to test and verify the robustness of the new watermarking algorithm [5] the JPEG compression and other signal processing attacks were tested. The results are shown in Figures 5 and 6. Figures 5 and Figure 6 show the test result of the distortion test and cropping test respectively. The results indicated in Figure 5 (f) with VQ and PRNG are superior than the results displayed in Figure 5(c) and Figure 6 (f) with VQ and PRNG are performing better than Figure 6(c).

The above Vector quantisation test illustrated that the VQ technique provides the ability to embed the watermark in different sizes without degrading the quality of the host image and the retrieved watermark. PRNG provides watermarked images which are more robust against distortion attack by means of random shuffling the watermark before embedding the watermark in the host image.

VQ provides flexibility in embedding watermarks in different sizes into the host image. The proposed system has an improvement over the traditional watermark scheme where the watermark size has to be fixed. In this method VQ makes watermark technology more desirable for the digital watermarking systems.

The digital watermark is used to protect the intellectual property rights of the owner. Therefore the watermark has to be protected from malicious attacks. The PRNG protects the watermark from being replaced illegally by using secure keys to generate the embedding position of the watermark randomly.

5 Conclusion

In this paper a novel digital watermarking technique was presented which can embed the grey level image. In the proposed method the digital watermark is first quantised using VQ with LBG [1]

algorithm. VQ transforms the vectors of data into indices that represent clusters of vectors. Then the vector is decomposed into a series of binary digital images for implementing multiple watermarks. The decomposed watermark image is embedded into the DCT[4] domain by modifying DCT coefficient values. The technique presented here is a new technique that has the ability to hide up to 25 per cent of host image size data in the host image - 16 times more than other traditional DCT based watermark systems [2][3]. Section 4 shows the result of embedding watermarked image into different bits. The recovered images Boat and Elaine have high PSNR value and good visual quality. The test results from Figure 5 and Figure 6 prove that this digital watermarking system is robust in countering both JPEG and other signal processing attacks [5].

References:

[1] Y.Linde, A.Buzo, and R.M.Gray,"An algorithm for vector quantizer design," IEEE Trans. Communications., Vol, Com-28,pp.84-95,Jan. 1980

[2] G.Voyatzias and I.Pitas, "Chaotic mixing of digital images and applications to watermarking," in Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST'96), vol. 2, pp 687-695, May 1996.

[3] R.G. van Schyndel, A.Z. Tirkel, and C.F. Osborne, " A Digital Watermark," in Proc. 1994 IEEE Int. Conf. On Image Proc,. Vol II, (Austin, TX), pp86-90, 1994.

[4] N.Ahmed, T. Natarajan, and K.R.Rao, "Discrete cosine transform,",IEEE Trans. Comput., Vol, C- 23,pp90-93,Jan 1974.

[5] F. A. P. Petitcolas, R. J. Anderson, "Evaluation of copyright marking systems", Proceedings of IEEE Meltimedia Systems (ICMCS'99), vol.I,pp574-579, June 1999, Florence, Italy.

[6] M. Matsumoto, T.Nishimura, M.Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator, ACM Tran. On Modeling and Computer Simulation Vol. 8. No. 1, Jan pp3-30 1998.

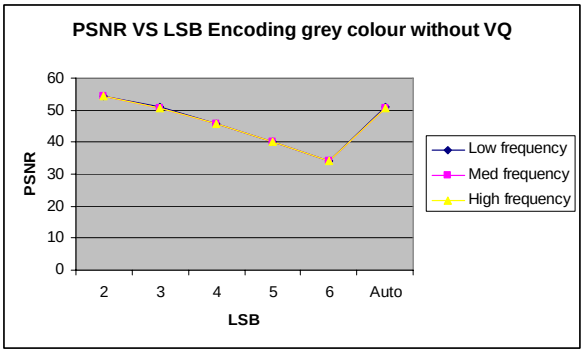

Figure 1. The image quality of the watermarked host image without using VQ & PRNG

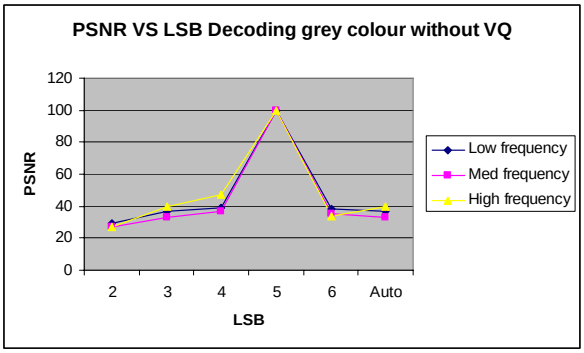

Figure 2. The image quality of the retrieved watermark image without using VQ & PRNG

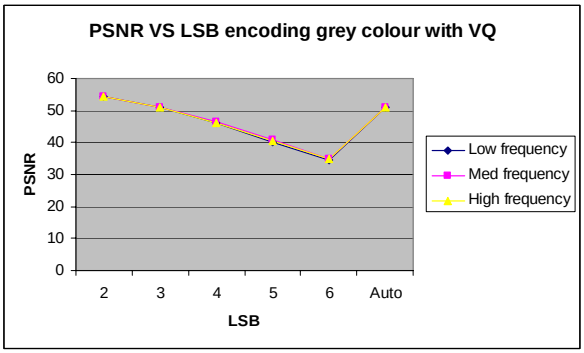

Figure 3. The image quality of the watermarked host image with VQ & PRNG

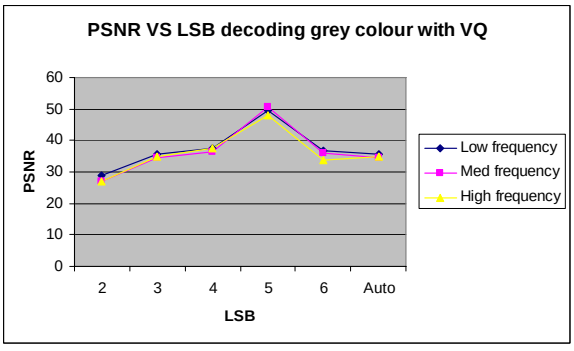

Figure 4. The image quality of the retrieved watermark image with VQ & PRNG

Figure 5 Distortion text test with binary watermark

Figure 5(a) watermarked image

Figure 5(b) watermarked image cropped

Figure 5(c) watermark image retrieved

Figure 5(d) watermarked image with PRNG + VQ

Figure 5(e) watermarked image cropped with PRNG + VQ

Figure 5(f) watermark image retrieved with PRNG + VQ

Figure 6 Cropping test for watermarked image without VQ and PRNG

Figure 6(a) watermarked image

Figure 6(b) watermarked image cropped

Figure 6(c) watermark image retrieved

Figure 6(d) watermarked image with PRNG + VQ

Figure 6(e) watermarked image cropped with PRNG + VQ

Figure 6(f) watermark image retrieved with PRNG + VQ