12-4-2013

Robust Watermarking Method By Systematic Block Diffusion Using Discrete Cosine Transform

Kazuo Ohzeki
Shibaura Institute of Technology

Kazutaka Bannai
Shibaura Institute of Technology

Yutaka Hirakawa
Shibaura Institute of Technology

Kiyotsugu Sato
College of Industrial Technology

DOI: 10.4225/75/57b3d850fb874
11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

ROBUST WATERMARKING METHOD BY SYSTEMATIC BLOCK DIFFUSION USING DISCRETE COSINE TRANSFORM

Kazuo Ohzeki[1], Kazutaka Bannai, Yuan-Yu Wei[1], Yutaka Hirakawa[1] and Kiyotsugu Sato[2]
[1]College of Engineering, Shibaura Institute of Technology, Tokyo, Japan
[2]College of Industrial Technology, Hyogo, Japan

Abstract
Digital watermarks have long been considered as a security feature. A watermarking method that involves the diffusion of limited watermark information into a large part of an image's data has high robustness. The diffused information is summed up to a single component before detecting the watermark. The summing up process eliminates small noises by an averaging effect, which improves the robustness of the embedded watermark against attack. In this field, thus far, only an asymmetrical Chirp transformation with a small block size has been attempted. In this study, a new verification experiment for a large block size of 256 × 256 pixels is conducted. High robustness of the proposed method is revealed. This includes the finding that, in the case of a JPEG compression attack, the proposed system is robust even at strong compression of 1/70. As for a clipping attack, embedded watermarks can be detected with up to seven-pixel clipping of an embedded image.

Keywords
Digital watermarking, Shrink, Diffusion, DCT, Systematic block diffusion, Clipping

INTRODUCTION

The use of digital watermarking for security or for proving tracking records in the field of image circulation has been studied. The robustness of embedded digital watermarks is the most important criterion for evaluation in important applications such as copyright proof and forensic authentication.

The robustness of digital watermarking itself is also currently being improved. If you reduce the number of information bits embedded in a watermark, then the embedded data have greater redundancy, so the robustness of the watermark improves. Ultimately, a one-bit watermark can be obtained (Ohzeki, 2005). The one-bit system at that time was a watermark for which the robustness of digital embedding was determined by a majority detection rule with embedding of the same information multiple times using the majority decision rule with a quantization method.

To improve the robustness, we introduce a diffusion method of the smallest watermark information elements into a large part of the data of an image plane. The diffused information data are summed up to a single component before detecting the watermark. Each diffused pixel element resists attacks at its position. Then, the surviving pixel data combine to provide positive watermarks during the summing up of diffused data.

The summing up process eliminates small noises by an averaging effect, which improves the robustness of the embedded watermarks against attack. In this field, thus far, only an asymmetrical Chirp transformation with a small block size has been attempted. In this study, a new verification experiment for a large block size of 256 × 256 pixels is conducted. In addition, we use discrete cosine transform (DCT) as a transform. The DCT is a very popular transform in the field of compression and watermarking.

ROBUSTNESS

One-bit watermarking

If more than half of the embedded values obtained in the quantization results exceed the acceptance/rejection level of 0.5, a majority will be satisfied, and the watermark determination will judge there was a watermark: information bit "1", which implies that the embedding was successful.

On the other hand, the result of there being no watermark, “0”, occurs if the number is sufficiently smaller than half; namely, the majority vote does not hold and no watermark is deemed to exist. Because 0.5 is the average value of these two states, 0.75, which is the mid-value between 50% and 100%, is considered a reasonable threshold. Similarly, the majority is negatively satisfied for results less than 0.25. The existence of watermark embedding is considered not to be certain when the determination result is in the interval between 0.25 to and 0.75. For such a case, we conclude that there was no watermark embedding. Therefore, as the determination result may have three states, namely, definitely successful, uncertain and definitely unsuccessful, it cannot be configured into just two states (1 and 0) and less than this, the 1 state, nor the 0 state. Furthermore, when a watermark is embedded, if the determination result can be classified into the 0 or 1 state, the watermarking is called “one-bit watermarking.” In other words, the state of “0-bit watermark” (Furon, 2005) does not exist as we can determine only whether the watermark was embedded or not know whether there was 0/1 bit embedded. On the basis of this one-bit digital watermark, in order to strengthen watermark robustness, the following were developed:

1. Majority method (Ohzeki, 2005): In this method, considering a large number, a representative result of a decision derived on the basis of the majority decision is detected.
2. Spread spectrum (SS) method (Hartung, 1999): This method divides a signal into its frequency components, embeds watermarks and then integrates the components back into the signal.
3. A Viterbi decoding scheme (Bas, 2007): This reaches a soft decision on the basis of a large number of embedding results; it is determined by using the Viterbi decoder.

Systematic block diffusion method

The Spread Spectrum (SS) method uses high-frequency components (Hartung, 1999), which are rarely available in image data. Image data share low-frequency components much more than high frequency. Therefore, the SS watermarking tends to be fragile. To improve the robustness, a systematic diffusion method was developed. The diffused data is systematically collected to a single element in each sub-divided region of an image. These collected elements are further processed by an orthogonal transform, DCT.

There are methods to maximize the redundancy of information in a watermark in order to enhance its robustness. In such methods, there is considerable redundancy because the same information of the watermark is embedded into multiple elements, in contrast to the methods that embed a single watermark information bit into a single element. Furthermore, they have the potential to be significantly robust. Some of these methods are listed in Table 1 with the quantization level serving as the criterion for robustness. The quantization input and output relationship for level “Q” is shown in Figure 1. The quantized values have two settings of zero and one. One means that there is a watermark, and zero means that there is not. The larger the quantization level Q, the stronger the robustness. The cell labelled “Individual” indicates that the watermark is detected individually for each element. “Block” indicates that the watermark is detected by using several data values in a block. In the Viterbi method, by pending determination of an individual, the maximum likelihood method for multiple elements is used. However, there are judgment criteria of each individual element. If the error is small, a soft decision works effectively. However, there is no effect of likelihood methods for large error. In the systematic diffusion method, multiple elements are integrated by adding them before the determination. The embedding information is detected successfully after expanding the threshold of the detection. The quantization levels of the decision are expanded to the number of pixels N × N that are diffused. Therefore, the robustness of the watermark embedding increases considerably. Digital watermarking using orthogonal transformation has a typical structure with substantial robustness because the value of the watermark embedded in the low-frequency

Method	Decision	Quantization Level
SS	Individual	Q/2
Majority Decision (Hard)	Individual	Q/2
Viterbi	Combined Soft Decision	Q/2
Systematic Diffusion	Block	Q/2 x N x N
Orthogonal Transform	Individual	Q/2

Table 1 A Comparison of Robust Watermarking Methods

component diffuses across the entire block. However, since the configuration has a single-element basis, the robustness of the watermarking system is limited. In the systematic block diffusion scheme, this effect works in two stages and leads to significant robustness.

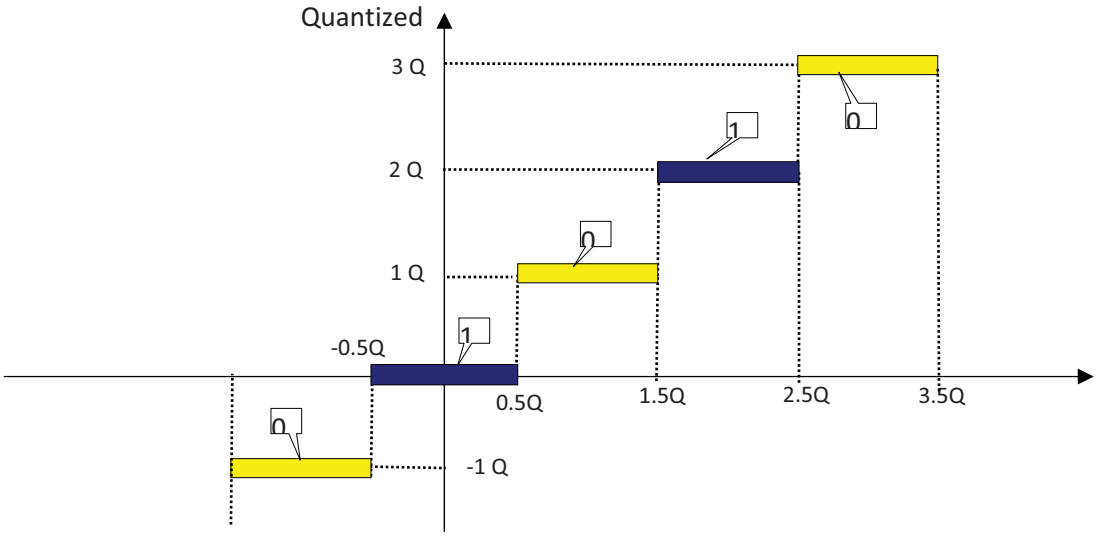

Figure 1 Quantization for watermarking as embedding operation

Proposed Method

In this chapter, we describe thesystematicblockdiffusionmethod. A block diagram of the embedding is shown in Figure 2 and a flowchart in Figure 3. Furthermore, a flowchart of the detection is shown in Figure 4. Note that the basic configurations of the systematic diffusion scheme are given elsewhere (Ohzeki, 2012_1,2). However, because the block sizes in these configurations are small and the Chirp transform has been used in the literature, the scheme did not exhibit the best performance. In this study, we have used a sufficiently large block size and DCT for verification of the above-mentioned diffusion method.

First, this method reduces the size of a luminance image after colour space conversion. The image formed by this process is referred to as a reduced image. Let the width of the reduced image be M and the height be N. Let α, β be the size ratio of the horizontal and vertical dimensions, respectively. Then, let the width of the luminance image be αM and the height be βN. Next, DCT is performed on the reduced image in order to convert it into the frequency domain. Then, by quantizing the DCT coefficients, we embed the watermark information. Next, after carrying out the inverse DCT, a reduced image in which the watermark information is embedded is generated. This reduced image is then expanded to the image of luminance with a quantized watermark having the size of αM × βN. The image thus expanded is called the expanded image.

Next, in this method, we calculate the difference of each pixel between the luminance image and the expanded image with a quantized watermark and then calculate the average value from the difference for each expanded range α × β, which is referred to as an average block. In the final stage,

we add the average value to the luminance image. After the above processing, a single watermark embedded in the reduced image is diffused in a block with α × β pixels.

This method involves the following procedure for watermark detection. First, we perform colour space conversion from the RGB system into the YCbCr system in order to create a luminance image composed of only the luminance component. Then, we perform a reduction with the same ratio as making the reduced image in orderto expand the watermark. Through this reduction, we retrieve the information diffused in the block of α × β. Thereafter, we perform the DCT on the reduced image. Finally, we extract the DCT coefficients from the positions at which they were embedded in the embedding process. We detect whether the quantized value is 0 or 1.

Another example of the configuration of the embedded block is shown in Figure 5. This method is carried out at the stage of the reduced image processing in order to calculate the difference between the original image and the reduced image. Furthermore, the expansion is carried out later. Thus, the content of the difference signal becomes clear. Both the methods expand the difference image, but they do not add the difference image to the original image as is. In order to avoid truncating the fractional component of the difference, errors are allocated to the original image so as not to increase the errors and to keep them to less than the least significant bit (LSB).

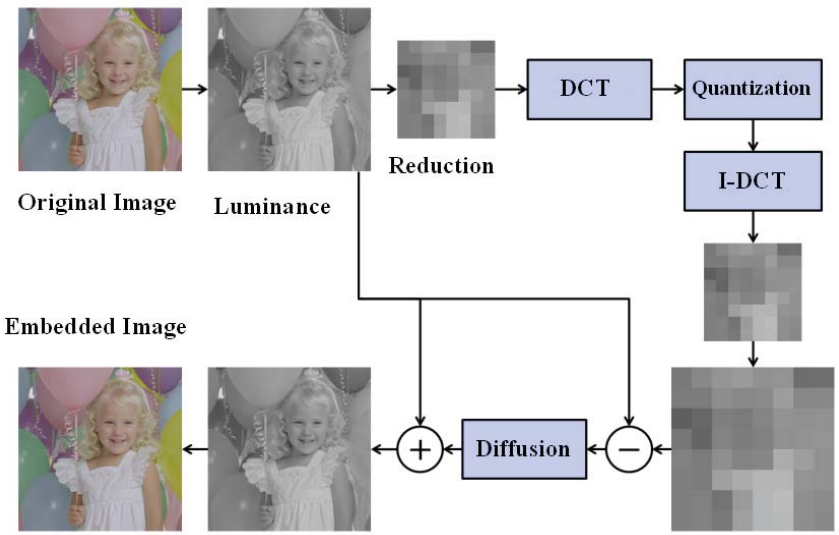

Figure 2 Embedding Block Diagram of the Proposed System

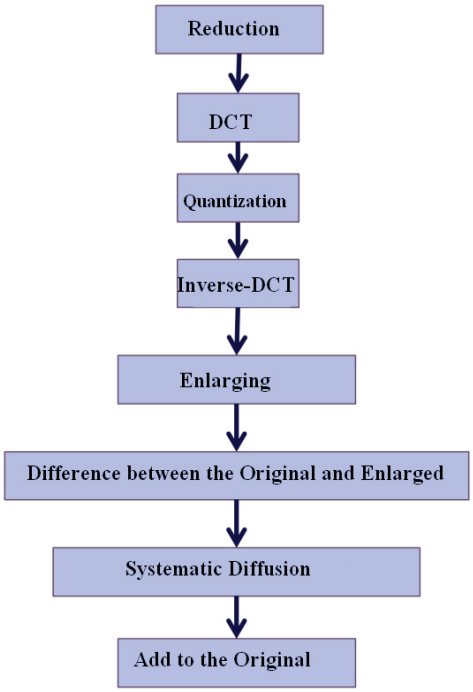

Figure 3 Embedding Flowchart of the Proposed System

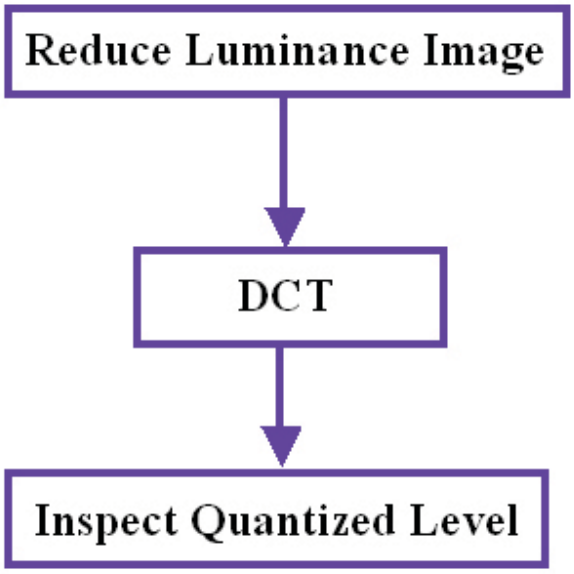

Figure 4 Detection Block Diagram of the Proposed System

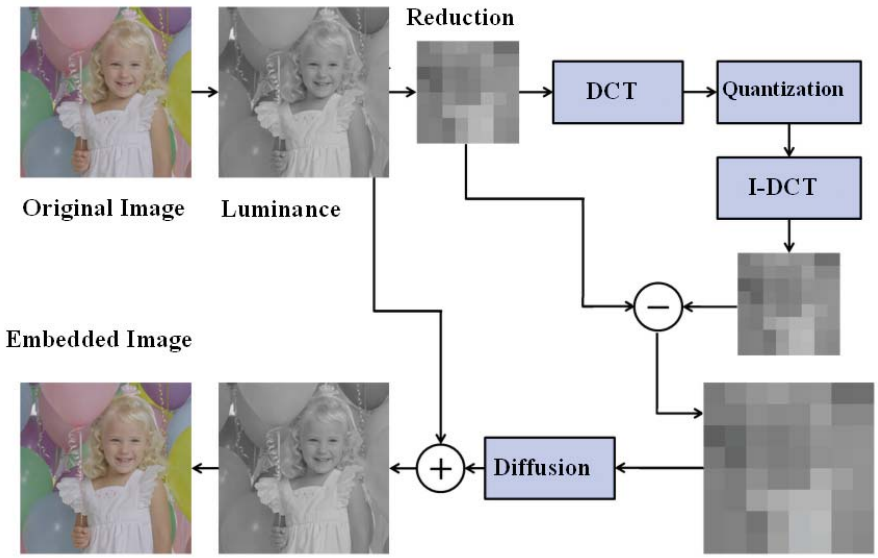

Figure 5 Another Embedding Block Diagram of the Proposed System

EXPERIMENTAL RESULTS AND DISCUSSION

Experiments with the above configuration were carried out. For the systematic diffusion method, as described previously (Ohzeki, 2012_1,2), its efficiency was only investigated using a special format by Chirp transform of a small block. Hence, the general validity of the method was not proved. In this study, as the block size of the original image is expanded to 256 pixels, the reduction ratios are set to increase to $\alpha = \beta = 32$. Furthermore, as test images, including images that we captured, 12 standard images published in the standard image database (SIDBA) are used. These images are 256 × 256 pixels in size, and are in the 24-bit full-colour bitmap format.

The experiments are performed using the original image described above, by using the watermark embedding device with the proposed systematic diffusion method. In the reduction process, the image is reduced to an 8 × 8 pixel image; that is, the reduction rate is 3.125%. Moreover, it is assumed that one bit of information is to be embedded. The embedding position is set at (1,0) in the DCT transform domain. The quantization level for the embedding is one of six values (8, 16, 32, 64, 128 and 256). A summary of the parameters is given in Table 2.

0

Table 2 Embedding Specification

Items	Specifications
Image File	Full-colour 24-bit bitmap
Image Size	256 x 256 pixels
Reduced Image Size	8 x 8 pixels
Reducing Ratio	3.125% (1/32)
Embedding Information	1 bit
Embedded Position in DCT Region	(1,0)
Quantization Step Size	(8, 16, 32 64, 128 and 256)

Robustness against JPEG attacks

Figure 6 shows the detection rate of a watermark after a JPEG compression attack. The horizontal axis is the compression ratio of the sizes of the compressed and original images.

From the results, 100% detection of the watermark is achieved in the compression up to 70% (0.0143). Compared with a previous trial experiment for a small block, in which the performance was

approximately 1/15 (0.0667), a large improvement is obtained. The original image (a) and the image compressed to 1/70 (b) are shown in Figure 7, where (b) is the embedded watermark with Q = 8. In the case of Q = 8, degradation due to watermark embedding is very small and can be neglected for subjective evaluation, as described below.

0

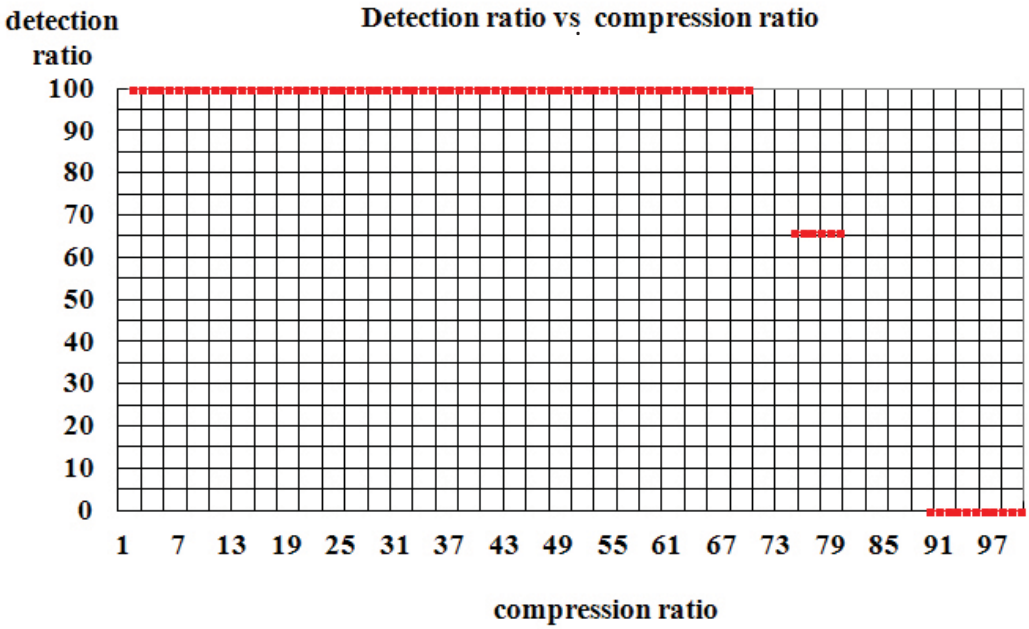

Figure 6 Detection Ratio after JPEG Compression of 1/70

In Figure 7, we can see that the robustness for JPEG compression of 1/70 is sufficient for practical use.

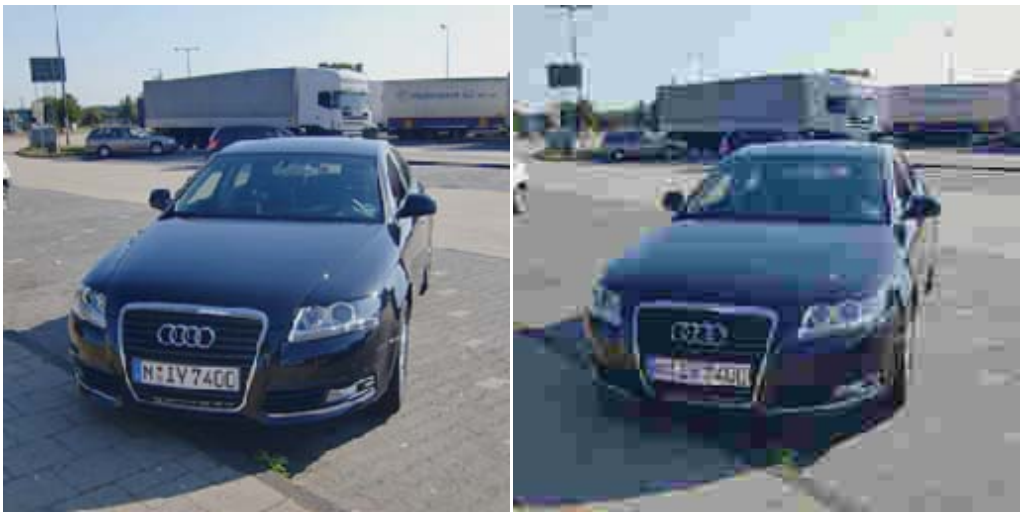

Figure 7 (a) Original Image (b) JPEG Compressed Image at 1/70 with Embedding at Q = 8

Robustness against clipping attacks

In the systematic block diffusion method, because one element of the watermark is diffused into the data of a large block, the robustness against attacks increases. The detection results against clipping attacks are shown in Table 3. Clipping is performed by cutting out S pixels from the right and bottom edges. Since detection is carried out in a 256 × 256 pixel image, processing of the uniform enlargement to 256 × 256 pixels is performed before detection. From the results, 100% detection is

achieved for all six quantization levels of Q = 8 to 256 after the clipping of seven pixels, as shown in Table 3.

Table 3 Robustness against Clipping Attacks

Number of Clipped Pixels	Number of Detected Watermarks of Q = 8... 256
1	6
2	6
3	6
4	6
5	6
6	6
7	6
8	0

Error evaluation

Degradation due to embedding is evaluated using the S/N. Figure 10 shows the distribution of the S/N versus the quantization level. The images considered are 12 images in SIDBA. The points in Figure 8 show the PSNR of each image, and the line represents the average of all the images. For the quantization level of 128, PSNR is less than 35 dB and degradation may be perceived. The quantization level of 64 or less has PSNR of more than 35 dB and can present good quality without perceived degradation. Furthermore, in the case of Q = 8, degradation due to embedding cannot be detected visually.

When the quantization level is 64, sufficient robustness is assured. Furthermore, since the average of PSNR is more than 40 dB, the embedding is considered highly robust and degradation cannot be observed for most images.

CONSIDERATION FOR FORENSICS

Some examples of fusion as part of e-forensics are methods for estimating a camera model from the data analysis of photos (Cohen, 2008) and estimating the changed features when altered photographic data are presented (Sorell, 2008). It is believed that practical digital watermarking can be used not just for evaluating an image or

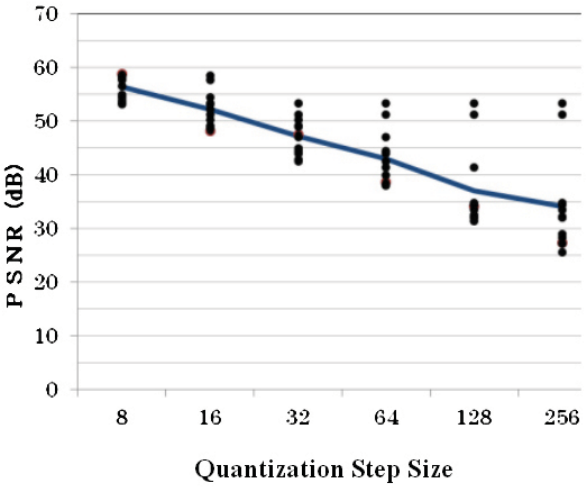

Figure 8 Signal to Noise Ratio (S/N) for Different Step Sizes

some media alone, but also for evaluating the environment, and obtaining information such as issues related to the owner and the route by which the media were obtained.Hence, it is not necessary for digital watermarking to havecomplete authentication ability. There is value in the method, as long as it has an authentication possibility of more than 0%.

Figure 9 shows various kinds of evidence for authentication, with the horizontal axis representing the existence probability. It can also be pointed out that a cryptograph cannot always ensure safety because it is only computationally complex and the safety level can be estimated by probability. Furthermore, in the Secure Socket Layer (SSL), at a practical level, that of approximately 128 bits is unsafe, at least by itself. It is protected by the many parts that encompass it. Now, even though the watermarking technique does not guarantee safety by itself, its practical application is valid by restricting the situation in the scene in the case or by reducing illegal profits and increasing the decryption costs of decoding for attackers. Watermarks for image processing software for digital cameras will be used more in the future, as shown by the examples of Cohen (2008) and Sorell (2008).

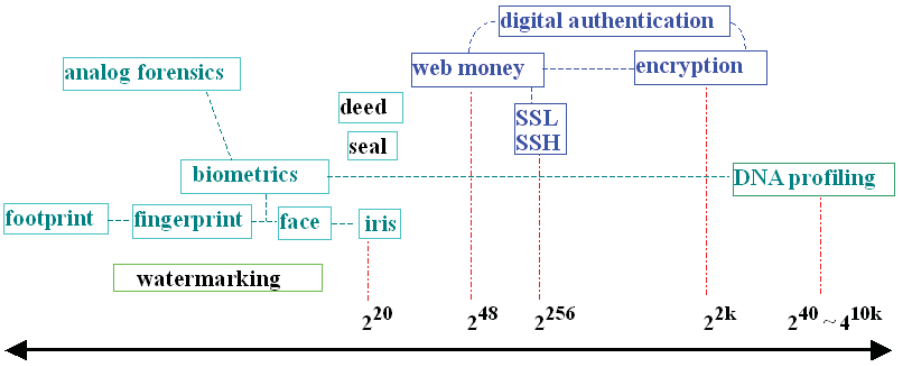

Figure 9 Examples of analog and digital evidential matters(Ohzeki, 2011).

CONCLUSION

DCT and systematic block diffusion enabled the improvement of embedding performance. By using the enhanced scales of 32 × 32-fold diffusion, we achieved a significant improvement in robustness. In the case of an attack of JPEG compression of 1/70, detection was successful for all quantization levels. Furthermore, in the case of a clipping attack by cutting the surrounding area of the image, the proposed system was robust for clipping processing up to seven pixels. However, detection was not successful for eight-pixel clipping.

Two different operations for obtaining watermark components in the proposed systematic diffusion were found to have the same characteristics. Significantly improved robustness was obtained for the proposed systematic block diffusion, compared with the DCT QIM conventional method, because it performed the embedding as a large two-stage reduction process. On the basis of the improved basic robustness, we can expect that the use of digital watermarking will increase.

REFERENCES

Ademola O. ADESINA, Henry O. NYONGESA, Kehinde K. AGBELE. (2010, May).Digital Watermarking: A State-of-the-Art Review.IST-Africa 2010 Conference Proceedings pp.1-8.

Barni, M. et al and Moulin, P. (2003, Nov). What Is the Future for Watermarking? (Part II). IEEE Signal Processing Magazine, Volume: 20 Issue: 6, pp.53-57.

Bas, Patrick, Doërr,Gwenaël (2007) Practical Security Analysis of Dirty Paper Trellis Watermarking, 9th International Workshop of Information Hiding (IH07) LNCS 4567 pp. 174-188.

Cohen, Michael. (2008, Jan.).Advanced JPEG Carving, Proc.First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2008) B3-1.

Digimark (2012, Sept.). Seventeen (Sept 2012) - 250 Digital Watermarks! Website: http://vimeopro.com/digimarc/discover-real-world-examples.

Furon, Teddy. (2005). A Survey of Watermarking Security. Lecture Notes in Computer Science, 2005, Volume 3710/2005, pp.201-215.

Hartung F., SU J. K., GIROD B. (1999, April) Spread spectrum watermarking: Malicious attacks and counterattacks. SPIE Proceedings Vol. 3657 ISBN: 9780819431288, 9.

Herley, C. (2002, Sept). Why watermarking is nonsense. IEEE Signal Processing Magazine, Volume: 19 Issue: 5, pp.10-11.

Ohzeki, Kazuo, Cong, Li. (2005, June). Consideration on Variable Embedding Framework for Image Watermark against Collusion Attacks.Wavilla Challenge (WaCha) 2005, Proceedings of the WAVILA Workshop on Watermarking Fundamentals D.WVL.2-1.0.pdf, pp.54-62.

Ohzeki, Kazuo, Wei, Yuan-Yu, Kuraki, Mao, Hirakawa, Yutaka,and Sato, Kiyotsugu.(2011, Dec.).A New Watermarking Method with Block Diffusion and Biased-Chirp Transformation. IEICE Japan Tech. Report Information Security ISEC2012_3.1 (in Japanese).

Ohzeki, Kazuo, Wei, Yuan Yu, Hirakawa,Yutaka, Sato, K. (2012, June) A New Watermarking Method with Systematic Diffusion and Biased-Chirp Transformation. Proc. ICCSET.

Ohzeki, Kazuo,Wei, Yuan Yu, Hirakawa, Yutaka, Sato, Kiyosugu. (2012, Aug.)Consideration of an inversion attack to watermarking and a countermeasure with a rounding operation.IEICE Tech Report Multimedia Information Hiding and Enrichment EMM2012-7 (in Japanese).

Ohzeki, Kazuo, Wei, Yuan Yu, Hirakawa, Yutaka, Sato, K. (2013, July). Two-Stage Watermark System for increasing Copyright potency in Image Media. Proceedings of e-commerce in IADIS, pp.93-95.

Ohzeki, Kazuo, Wei, Yuan Yu, Hirakawa, Yutaka, Sato, Kiyotsugu. (2013, Aug).Consideration of the Watermark Inversion Attack and its Invalidation Framework.Proc. of International Workshop on Digital-Forensics and Watermarking IWDW2012 doi 10.1007/978-3-642-40099-5_9.

Sorell, Matthew. (2008, Jan.).Conditions for Effective Detection and Identification of Primary Quantization of Re-Quantized JPEG Images.Proc.First International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2008) B3-3.

Zhang, Yanqun (2009, June). Digital Watermarking Technology: A Review. InternationalConference on Future Computer andCommunication, pp.250-252.