Watermarking using Side Information

A.Antony and M.A.Ambroze

Fixed and Mobile Communications, University of Plymouth, Plymouth, UK
e-mail: M.Ambroze@plymouth.ac.uk

Abstract

Digital Watermarking was developed so as to prevent the illegal use of the digital media. The extreme significance of it started when cybercrimes started to multiply. To a large extend watermarking was capable of preventing such misuse. However with the rise of threats to the watermarking, there was an acute requirement of some technological improvements so as to sustain the fact of securing digital data within the communication systems. The approach to solve this problem was by modifying the existing watermarking schemes corresponding to the levels of security and robustness. The main aim of this paper is to develop a watermarking scheme which has the properties of robustness to attacks and at the same time providing considerable amount of security. For this a research was conducted for attaining this objective and the results publicized that watermarking in the frequency domain can attain this criterion when compared with the schemes of watermarking in the spatial domain. So, a watermarking scheme, in discrete cosine transform (DCT) was experimented for this purpose on the frequency domain. This scheme was supposed to undergo geometric distortions like rotation and cropping. Finally the results revealed that this was really substantial in most of the cases to that of the schemes in the spatial domain like LSB watermarking mainly.

Keywords

Watermarking, Discrete cosine transform, LSB, Robustness, Security

1 Introduction

The very first discussion about the watermarking was made in the year 1979, as a unique method for the production of machine detachable patterns and signs to recognise anti-fraud and anti-counterfeiting activities (Szepanski, 1979). Though this was not been adopted for any real life applications, after around nine years a study was published where an identification code was embedded on an audio signal and this was the very first time that the phenomena of digital watermarking was brought into applying on it (Bani and Bartolini, 2004). From there on there had been tremendrous outbreak of the papers. The growing numbers of papers had been increasing exponentially since 1990 (Cox *et al.,* 2002). This implies that plenty of applications related to the digital watermarking was been wide spread.

Normally in a watermarking process a watermark is added to a cover object to form up a watermarked image. The sender and the receiver share a secret key in order to make this communication secure. However, Steganaography can be classified based on two types they can be either fragile or robust. Fragile schemes of watermarking are easily destroyed if any variation happens to the watermark inside. But, the robust watermarking schemes are capable of resisting this (Cummins *et. al*., 2004). Based on accruing this specifically the detection mechanism must be efficient.

In this paper, the research was concerned in analysing on the steganographic watermarking using the informed detectors. Normally, detectors used are of two types they can be Informed or Blind. Informed detectors are the ones in which the watermarking information is known to the sender and the receiver (Al-Houshi, 2007). So the only work that is involved with the receiver is that it has to compare with the original cover image, when it is supposed to check for the presence of the secret. Hence, the factor of complexity involved is much less.

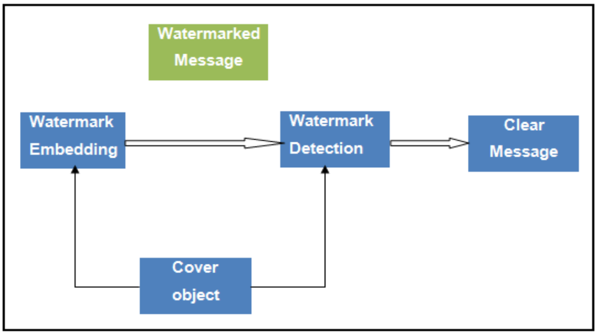


Figure 1: Watermarking using Informed Detctors

In the research we conducted, we where expected to find out a method that could considerly have robustness and security at the same point. The investigation started by analysing on the Least Significant Bit hiding method in the Spatial Domain.

Considering the LSB coding, it is also known as bitpalne coding. In this it basically tries to encode secret information by substituting the secret information on the insignificant parts of the cover. The receiver can extract it easily if he is aware of the secret and knows the positions where exactly it is embedded. Here only very minor modifications are made and it is all upon the assumption that it wont be noticed by the a passive attacker. Our research handled on Bitmap files as, there won't be many losses involved and hence data can be easily manipulated and recovered.

Now analysing of the LSB substitution, it is used on one bit on a very minimum case and that is expected to be distributed over the cover when it is embedded. Which means there will be change in *Ci* (cover image) due to message, *Mi* (*Mi* is either 1 or 0). However this becomes slightly efficient when it uses more bits when swapped with the cover and the secret. Finally in the process of extraction, the LSB of the selected cover elements are extracted and lined up to form the secret. In the process of decoding, the receiver must be capable of knowing how many elements are to be used in the embedding process. In a very simple case what really happens is that the sender would be using all the cover elements to make the substitution starting from the first element. As the secret is having really less number of bits than the l(c) (length of the cover), the embedding process gets over long before the end process of the cover. So, there are possibilities of some cover elements getting unchanged. Now this is going to be a serious issue creating security problems. To overcome the above mentioned issue it is enough to make the length of the cover and the secret to be the same, i.e., l(c) = l(m)

Now when this is done there will be changes in the number of elements for transmission. When this happens there will be a suspicion in the mind of the attacker and may make him think that some secret is getting exchanged since there is a slightly high variation in the bandwidth consumption.

Hence, another sophisticated approach is the use of psedorandom number generator for spreading the secret message. If both the sender and receiver share a key *k*, used to generate numbers, it will be much efficient to a certain level reducing the level of getting attacked (Katzenbeisser and Petitcolas, 2000).

Now the limitation still existing is the impartment of attacks over this kind of technique. LSB watermarking is not at all resistant to any kind of attacks. Hence there is no phenomenon of robustness involved in them with very less amount of security. So, the research had to take up some other measure so as to improve the above facts.

As this was analysed the research had to turn up towards some other watermarking scheme which could hold attacks. Analysing deeply it was found that the Frequency domain techniques can hold attacks much effectively. Hence a watermarking scheme in the frequency domain was formulated namely the Discrete Cosine Transform.

2 Testing Methodology

Watermarking in the Discrete Cosine Transform is one of the popular hiding technique which works in the frequency domain. In this the relative size of the coefficients is taken into picture. As per the concept we can take two or more of these coefficients. However in this research it has taken up just taken up two coefficients. Again the research is considering a system which makes use of digital covers. This is quite similar to the proposal by Zhao and Koch (Zhao and Koch, 1995).

The investigation is taken into account of a cover communication where a secret is shared in the form of an image between a sender and a receiver. For this in the sending part, we are splitting the cover image into blocks of 8 X 8 pixel and each of these blocks encodes exactly one secret bit every time. Again, in the embedding part we will be selecting a particular block and this will be considered to be in of the same nature. For example if the embedding starts with the selection of a sequence b_i which is used to code the message bits then we can then calculate the discrete cosine transform of the blocks easily using the formulae ,$B_i = DCT\{ b_i \}$.

Now as per the concept the sending part and the receiving part is supposed to agree in the location of the 2 particular coefficient values in DCT which is to be used for the purpose of embedding. If we are taking up those coefficients to be (u1, v1) and (u2, v2) there are many criteria that these coefficients must satisfy. They must correspond to the cosine functions and must be with the middle frequencies. Doing this ensures that the information or the secret is contained in the significant parts of the image or the cover. Again the intension behind this is that the secret wont be destroyed by the compression taking up. Hence to maintain robustness to the newly formulated system, it is essential to select the DCT coefficients with equal quantization values.

As per the algorithm, every time a block satisfies the condition B_i (u1, v1) > B_i (u2, v2) it is “1”, otherwise it holds the value “0”. In the process of encoding, the two coefficients are been swapped if the relative sizes of those two coefficients is much less when compared to the bit to be encoded. By doing this it can affect the relative sizes of the coefficients and during compression the algorithm here make use of a condition and add on some random values for both of the coefficients such that $|B_i$ (u1, v1) - B_i (u2, v2)$| > x$ for every $x > 0$. Here x in this case is assumed to be the gain, higher the value of x corresponds to higher amount of the robustness in the compression. Then the sending part will take the inverse DCT to convert it from the frequency to the space domain. In the decoding section the image is DCT transformed initially. Then making a comparison over each block, i.e., searching for the two coefficients over every block the secret can be restored. If the value of ‘x’ and the coefficients are selected properly then there will be robustness in the image obtained. The detailed algorithm of implementation of both encoding and decoding is mentioned below.

But the most notable drawback of this system so far analysed is that it wont discard any of the blocks where the relation of the DCT coefficients are not satisfied. In such a case there will be considerable damage in the image (Johnson and Katzenbeisser, 2000).Now the theories say that there is pretty large amount of robustness involved in this using the substitution method. Now the question is how we can measure it. It can be done by implementing attacks over this watermarking scheme.

The DCT watermarking can be done making use of the logic above, now the robustness of that can be calculated, by making some geometric distortions on them. Analysing the fact that small geometric distortions can create distortion to the secret message and prevent in the detection of the watermark (Lin *et. al.,* 2001), the marked cover is been experimented by rotate and crop.

For the purpose of this initially, we did the watermarking in the DCT domain and studied the variations that happened. Analysing them attack where implemented on them. We took a 512 X 512 standard grayscale image of lena as the cover and a black and white secret image as the secret. The framework used was matlab R2007a.

3 Results and Discussions

Results obtained in the case of the normal DCT watermarking was not that different from any of the spatial domain schemes. The usage of informed detectors, vanished the problem of receiving adequate robustness in the subjected methodology. However, there was variations in the secret and the cover when they where subjected to the rotate and crop. Although the cover didn’t have considerable amount of variations apart from the normal problem of loosing the luminance coefficients, the variations in the secret was dramatically, increased when rotated for higher angles and cropped with different coefficients.

3.1 Rotating the cover

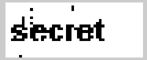
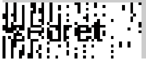
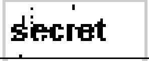
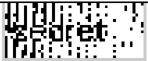
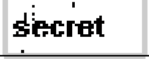
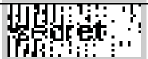
Sl No:	Angle in (Degree)	Rotating Clockwise	Rotating Anti-Clockwise
1	0.012		
2	0.05		
3	0.1		
4	0.5		
5	1		
6	5		

Table 1: Secret image modifications with rotation of cover

In rotation the watermarked image is subjected to rotate over an angle. As told earlier in the background, the watermarked file is created by randomly swapping pixel coefficients. Now when rotation is done what specifically happens is that, there involves a "cyclical shift" in the coefficient values which was used in watermarked by swapping (Lin *et al.,* 2001). This fully corresponds to the unequal displacement of the secret image in this case. Now, retrieval of the secret image is really hard at the time being as the coefficients swapped are fully out of order when considered with the initial arrangement. Although if it is the case, if the watermark or the secret image is tried to recover at this point, it is sure to have errors on it. In simple words, it can be assumed that the watermark is expected to be fully degraded. Now the question at this point is how the research did managed to get some visible part of the secret image with very slight errors. This is because, before detection of the secret image it is subjected to be "resized" to the normal size of 512 X 512. This proves that robustness is less when rotation is done but, the watermark can be extracted with minor errors considerably on very small or finer angles. Experimenting on larger angles is reveals that there is no part of the secret that could be retrieved. This is because there is a maximum limit to which recovery of the image can be made with the point of rotation. From around 500 executions made these results were analysed. Again another point to be discussed is why degradation is more in the case of anti-clockwise rotation when compared to the clockwise rotation. This is because rotation is combatable more in one direction alone and not in the other direction (Lin *et al.,* 2001).

3.2 Cropping the cover

In the initial observations of the outcomes on the survival of watermark, it is understood that when the coefficients are given as input with minor variations from the standard size of the image, then the watermark survives.

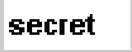
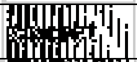
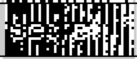
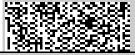
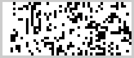
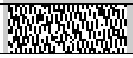
Sl no:	Pixel Coefficients (used for cropping in the Rect function)				Secret Image Recovered after Cropping
	X_{min}	Y_{min}	Width	Height	
1	1	1	510	510	
2	2	2	508	508	
3	3	3	511	511	
4	250	250	500	500	
5	500	500	500	500	
6	512	512	512	512	
7	64	250	500	500	

Table 2: Secret Image modifications with cropping

As per the results, only in case 1 shown in table 2, this is the only point that a watermark has survived reasonably well. The explanation to this is generally that the pixel coefficients randomly used in the DCT watermarking in the frequency domain is not disturbed much. The watermark survived just because the randomly distributed pixel coefficients used in DCT is almost in the center of every block. As long as this is not disturbed there would not be any other considerable variation. In all situations the degaradation is more. While cropping, a function called the 'rect' in matlab was used to take pixel positions as the input. Now, the notable point is that, depending on the values given as input there will be variations in the cover and the watermarked image. In case 7, it is observed that the cover image is been scaled, although the watermark is completely degraded. If the cropping of the image is not symmetric when considered on both rows and columns, then there will be scaling of the image to a "canonical size" with an associated "translational shift" (Lin *et al.,* 2001). This is the reason for scaling of the image, when cropping was performed at this point as the geometric attack.

4 Conclusion and Future Works

The results that we got in the case of rotation and cropping significantly proved that the DCT watermarking had potentially higher resistance in the case of robustness and security, when compared to the spatial domain techniques like the least significant bit hiding. Although the research fundamentally aimed in getting a centum performance on acquiring robustness and security, another prime objective was to work on the watermarking with side information which was not yet achieved due to the limitation of time and the pace of research. To make this possible, more investigations must be done in the principles of spread spectrum techniques of watermarking and on concepts to improve, for bringing blind detectors to work like informed. Error analysis can be further done on the scheme that we have proposed, if this is done significantly well then, there will be more effectiveness achieved of this proposed model. Investigations even should be done regarding the experimentations of using different cover images including different colour patterns. If attacks are done more than one at a time, is yet again a possible area to be researched into.

5 References

Al-Houshi, (2007), ‘Watermarking using Side Information’ MSc. Thesis, University of Plymouth

Barni, M., Bartolini, F., (2004), ‘*Watermarking Systems Engineering: Enabling Digital Assets Security and other applications’.* New York, USA

Cox, I J., Miller, M L., Papathomas TV., (2002) ‘*Digital Watermarking*’ London, UK: Morgan Kaufmann.

Cummins, J., Diskin, P., Lau, S., Parlett, R.,(2004) ‘*Steganography and Digital Watermarking*’ School of Computer science, The University of Birmingham.

Katzenbeissser, S., Petitcolas, F., (2000) ‘*Information Hiding Techniques for Steganography and Digital Watermarking*’ Chapter 3: Survey of Steganographic techniques Page nos: 43-74 Artech House, Boston, London

Lin, C. Y, Wu, M., Bloom J.A., Cox, I. J., Miller, M.L., Lui, Y. M., (2001) ‘*Rotation, Scale, and Translation Resilient Watermarking for Images*’ IEEE Transactions on Image Processing, Vol. 10, No.5

Sepanski, W., (1979) ‘*A signal theoretic method for creating forgery-proof documents for automatic verification*’ Proceedings of Carnahan Conference on Crime Countermeasures (May 16-18, 1979), by John S Jackson Page no: 101-109

Zhao, J., Koch,E., (1995) ‘ *Embedding Robust labels into images for copyright protection’*, in Proceedings of the International Conference on intellectual property rights for information,knowledge and new technique, Munchen ,Wein: Oldenbourg Verlag, 1995,pp 242-250