Scientific Research and Essays Vol. 7(34), pp. 3032-3039, 30 August, 2012
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE12.195
ISSN 1992-2248 ©2012 Academic Journals

Full Length Research Paper

Study on watermarking effect in image-signature association copyright protection model

Mohammad. Al- Rababah[1]*, Abdulsamad Al-Marghilan[1], Mohammed Mosa Al-shomrani[2] and Mamoun Sulaiman Al-rababaa[3]

[1]Faculty of Computing and Information Technology, University of Northern Border ARAR, Kingdom of Saudi Arabia.
[2]Faculty of Science Math Department, University of King Abdulaziz, Kingdom of Saudi Arabia Jaddi.
[3]Dean of Computer Science Department Faculty of Information Technology, University of Al al-BayuT Jordan-Amman, Jordan.

Accepted 7 June, 2012

This paper aims to compute the effect of the different watermarking techniques on a proposed scheme of image copyright protection. This scheme depends on image association principle rather than image data modification. Hence, it is intended to support the developed technique with essential study to approve the validity with convenient measures and performance criteria. The effect of watermarking is classified in accordance to image format types. In this, distinguished rates of image disturbance are supposed to be injected as noise in either single component or multi components of image colour space attributes. The conducted experiment studied the effect of this noise on output associated signature using neural networks and Matlab. The study also extends to cover some suggestions that can be used as a diagnostic process to discover the intruding techniques from one side. And from the other side is to recover images from the resulting disturbed output resulting from traditional processing, like size and rotation affections towards robustness characteristic preservation.

Key words: Watermarking techniques, copyright protection, signature.

INTRODUCTION

Watermarking is a process in which a signal is hidden or embedded into another signal, usually a photograph, video, or music. There are a variety of possible uses for embedded signalling, ranging from covert signalling applications that encompass classical steganography, to recent commercial interest in providing copyright and copy control information. Despite the many developed techniques proposed for designing watermarking processing, broadly speaking there are two approaches used to modify the multimedia cover for the sake of embedding watermarks, The first approach denotes the spatial domain mode, in which the watermarking technologies modulates the original (cover) image intensity and the second approach on the other hand denotes a transformation or frequency domain mode in which watermarking embeds the watermark into the transformed image and not the original one. This classification supports the categorization in accordance with the domain for watermarking as a hosting environment (Mn-Ta and Shih-Syong, 2010).

Obviously, watermarking techniques in general had approved a successful tool in image copyright. Nevertheless, scientific trends do not restrict their efforts in these techniques. Different schemes have been presented (Hsiang-Cheh, 2008; Aditya et al., 2010; Mn-Ta and Shih-Syong, 2010; Charlie and Behzad, 2009). Besides these efforts, a newly presented study under a title of “Digital Signature Generation for Image Copyright Using Neural Network Global Data Association “is proposed. In this paper traditional data injection of the watermarking techniques is replaced by external association of image data and its related information from one side and a digital signature from the other side. Hence, no data regarding the image is altered or modified.

*Corresponding author. E-mail: hamzehamerah@yahoo.com.

Watermarking characteristics and requirements

Invisible watermarks are a proposed solution for the protection of Intellectual Property Rights and for dealing with the problem of illegal reproduction of multimedia objects. Numerous watermarking schemes have been proposed and implemented, but their performance evaluation, as well as their comparison, is a difficult task. Broad claims have been made about the "robustness" of the watermarking methods. Recent attacks have proven that the robustness criteria used so far are often inadequate. Most of the watermarking systems are made to be robust against JPEG compression, cropping, low-pass filtering and rescaling, but fail to succeed in simple geometric transformations and distortions like rotation. Consequently, there is a need for a robust watermarking method.

Watermarking mechanisms can be characterized by a number of requirements which are sought by any proposed application. It is worth mentioning that there is no single application that incorporates all the said requirements but various applications may incorporate different set of these requirements. The main expected requirements for watermarking can be summarized as below.

i) Perceptibility: The watermark image should be indistinguishable from the original cover image, that is, watermark should not distort or affect the cover image (Hsiang-Cheh, 2008), and thus it will be undetectable or unnoticeable except by the owner.
ii) Robustness: Watermark must be highly resistant to any distortion (intentional or unintentional), deliberate extraction of the watermark, modification, maneuvering etc. Furthermore, robustness might incorporate a great degree of fragility to attacks, in such a case; multimedia cover object is totally destroyed if it detects any tapering (Aditya et al., 2010).
iii) Integrity: No loss of original multimedia carrier.
iv) Accessibility: Both types of watermarking must permit for accessibility. Public type allows information handling for any interested entity to call attention to the copy/reproduction rights, while the private type necessitates extra authorization information in order to access the watermark.
v) Compatibility: Watermarked multimedia data should keep certain level of compatibility with the original data.
vi) Traceability: Watermarking can be repeated along a processing line in order to accommodate for multiple watermarks that reflects the stage throughout a tracking process.
vii) Security: Watermarking accounts for the protection of ownership against forgery and unlawful threats.

The proposed model involves two procedures. The first can be summarized by adding the information to the image in a wider frame environment. Then, after sampling this frame into the same number of signature pixels using a key, those samples of pixels are then reshaped to generate an array analogous to the dimensional distribution of the digital signature that is, in same column and row sizes. The resulting array is considered as input patterns used to set a training table. The output of this table is organized with the digital signature itself. This procedure stands for watermarking imbedding procedure. Hence, a neural network is used to associate the given input with the required output of the digital signature and after training the structural attributes of the neural network are saved as a second key that is to be used along the second procedure along with the first key that is used for the sampling purposes.

In the second procedure, the image under verification is taken and appended with the claimed information to be fed to the sampling stage with the first key. The output of such sampled data is then applied as input to the second key which denotes the structure of the neural net to extract the output. This output is supposed to be the digital signature. When the signature emerges without any noise, it is considered as a great evidence for the ownership. But when this output is gathered with noise then verification fail for the ownership as evidence.

Various watermarking techniques have been proposed as image copyright protection tools. Although these techniques achieve diverse scales of success, the injection of data modifications is still under investigation. For this reason, a model of image-signature association has been suggested. The current paper expands the investigation of this model. The main investigation conducted, is to prove the validity of the model against the main seven characteristics of watermarking; perceptibility, robustness, integrity, accessibility, compatibility, traceability and security.

Application of copyright approval and requirements

So far, different techniques are explained. For each technique there are different requirements needed to be prepared and kept by the owner. These requirements are essential to prove the ownership. As these techniques are of various design principles, they necessitate the existence of some material, other techniques might not consider them important. In this work an analytical investigation is made along with two questions (Ali and Ahmad, 2010). The first is about the type of materials that are supposed to be saved and who is responsible to keep them. Whereas the second argues about who should perform the watermark detection procedure for the judgment task.

Regarding the first question, there should be two partners; the owner side and the legal authorized side. The latter has to keep the watermark along with the programs of watermarking embedding and extracting procedures. Although, storing the image is logical, but it

makes no sense to accumulate many copies of original images with huge sizes of data repositories. This in other words means high cost for little benefits. It also means hard additional efforts devoted by the partner for any new registration including checkup procedures to all of the old images. With these two drawbacks, owners would not find such protection fruitful as it adds extra expenses. Therefore saving watermarks only is economically and practically more efficient. In this case the resultant cost would be low with little efforts as well. The owner thus would be able to register few numbers of watermarks for less payment along with little efforts conducted by the second partner. The only burden here would be just to assure no similar watermarks have been kept earlier.

On the owner side, the original images are kept. As an ordinary matter, original images mean the skills and art; owners are proud to keep them in his repository away from the copyright requirements. Furthermore, the owner can be involved in selecting the preferable watermarks of his works. Unique watermark may be sufficient to be used for all the works of one owner. But as known, when a watermark is detected by a counterfeiter, the problem of extracting the watermark and its related algorithm would be also simple. As soon as the watermark is recognized, the counterfeiter can hack the database and remove all watermarks in the concerned images of the owner. In addition to the original image, the owner should keep away any private keys regarding the watermarking used techniques. These keys would be provided by the owner to the authorized partner when needed in the verification phase. Moreover, the owner should keep away all the executable forms of the watermarking algorithms used for the embedding and extraction techniques.

The second argument is related to the question of who should perform the watermark detection procedure. For sure the answer denotes the authorized partner with the cooperation of the owner and under a certain request. The detection procedure is conducted when there is a dispute between the owner and a claiming counterfeiter. In such case, a certified testimony would be issued for the benefit of the owner using the valid laws and rules adopted in the concerned country.

The overall process is initiated when the owner gets any doubt of an appearing image. He/she can immediately check it by applying the related programs. When the owner manages to extract his watermark, a case is initiated for a court problem. Court in turn would call the second partner, the authorized side. The authorized side would ask the owner to have the private keys of the related images. With these keys, the authorized side would be able to extract the watermark in front of the court. When the process runs positively for the owner, the laws and rules would be applied to give the right verdict in favour of the owner related to the associated punishment to the counterfeiter including all the expenses of the whole case.

For research of the current work, it is necessary to detail the materials needed to judge on the ownership rights in accordance with the related partners of the process of copyright protection. Like the foregoing mentioned work above, the partners are the owner side and the authorized side. Here, the responsibilities and materials encountered can be envisaged as follows, while the detailed discussion related to these points will be thoroughly considered subsequently:

1. The original image: Obviously, the original image represents the art work of the owner; therefore this material is supposed to be kept by the owner. In fact, in the current work the original image does not abstract the image itself, but the information associated with it. This information represents the evidence used to prove ownership validity.
2. The private keys: In the current work the protection depends on two different keys. The first key denotes the random number generator seed. This generator is used to collect random samples from the image when being appended with its associated information. The second key represents the connection scheme parameters of a neural network feed forwarded configuration scheme. This scheme is used to associate the image and its information to owner signature. Both of those keys are supposed to be kept by the owner. Like the previous example, these two keys have to be provided to the second partner (authorized side) when the extraction process is executed.
3. Owner signature (logo): This material represents the signature of the owner. It could be designed by the owner as a binary image. Colour signature can be considered with the association structure. But for the sake of simplicity, the work adopted the binary image. The authorized side has to keep this signature in the database as registered evidence in order to verify the ownership rights when needed. This signature is not necessary to be of different models and styles. Unique signature is much better for the utilization purposes while the keys play the security role rather than the signature itself.
4. System algorithm programs: With a similar design, the whole process of image protection has two different programs. The first is termed as association program which simulates the embedding procedure of watermarking techniques. The second program is termed as the signature generator which simulates the watermark extraction procedure in watermarking techniques. In the current work, the first program can be attributed to the owner responsibility whereas the second program is kept by the second partner, authorized side. With the aid of owner information and the related private keys, the authorized arbiter is enabled to generate the signature. Figure 1 summarizes the partners and requirements of the presented image copyright protection proposal.

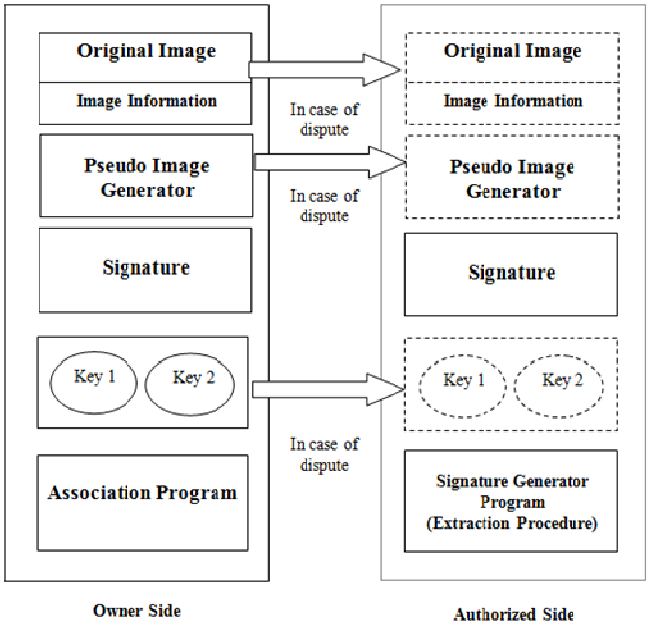

Figure 1. Model partners and requirements of the system.

WATERMARKING WORKS REVIEW

Despite the many developed techniques proposed for designing watermarking processing, broadly speaking there are two approaches used to modify the multimedia cover for the sake of embedding watermarks. This classification supports the categorization in accordance with the domain for watermarking as a hosting environment (Cox et al., 1999).

The first approach denotes the spatial domain mode, in which the watermarking technologies modulates the original (cover) image intensity. This watermarking technique requires simple and low computing complexity, as no other transformation is experienced. Designers usually strike a balance between robustness and perceptibility of the modulated image in order to cancel or reduce noise effect. For example, Kutter and Hartung (1999) developed a spatial domain watermarking algorithm that uses a string of bits and manipulates the values of the blue channel at single pixels that are visited in a zig-zag in order to get the sequence. Based on the same technique, Al-Nu'aimi and Qahwaji (2009) utilized the green channel as the host part of the image in order to achieve high invisibility and robustness due to the fact that it gives the best compromise between luminance and chrominance. Then, the watermark is reconstructed at extraction stage and compared with the original watermark. Another example of spatial watermark algorithm is developed by Rongen et al. (1999). It incorporates the use of the salient pixels for embedding the watermark. Their approach for watermark is shown to be robust to rotation, scale, and translation. Besides it has proved resistant to compression and cropping. The second approach on the other hand denotes a transformation or frequency domain mode in which watermarking embeds the watermark into the transformed image and not the original one (as in the spatial mode). This technique employs human perceptual behaviour and some frequency masking properties of human sensing systems for watermarking. Currently these transformation techniques are either discrete wavelet transform (DWT)], discrete Fourier transform (DFT) or discrete cosine transform (DCT) that transform the multimedia data to certain embedding locations. Therefore, this approach adds extra computational complexity as compared with the special mode.

Ali and Ahmad (2010) proposed a watermarking technique based on cascading two powerful mathematical transforms; DWT and the singular value decomposition (SVD). They embed the watermark bits on the elements of singular values of the DWT sub-bands audio frames. They achieved good levels of inaudibility and robustness assisting the copyright protection scheme that faces music business.

Tilki and Beeks (1996) employed a hybrid technique similar to amplitude-shift keying (ASK) and frequency-shift keying (FSK) for producing a 35 bits hidden digital signature onto the audio component of a television signal. It proved to be robust against most room noise.

Tao and Dickinson (1997) proposed an adaptive watermarking technique that assigns each spatial region a noise sensitivity label and embeds the watermark using block DCT according to its sensitivity label. The watermark detection threshold is chosen to achieve a desired false alarm probability, which we believe is an appropriate performance measure

Mei et al. (2009) reported a digital watermarking algorithm based on discrete cosine transform (DCT) and discrete wavelet transform (DWT). The watermarking that has been transformed as discrete cosine is then transformed as high frequency band into discrete wavelet. The reported algorithm results were invisible with good robustness for some multimedia processing operations.

PROPOSED APPROACH

The current research attempts to simulate a model in line with the foregoing traditional method of red wax based stamping. This model is referred to in this work as image association system. Where the image and its associated captured information stand for the envelop contents, signature stands for the bulge stamping and a neural network to simulate the envelop and the red wax together. Figure 2 gives the overall envisagement of the transformational view of this simulation modelling aspect.

In this concern, there is no need to inject any data inside the original image but to associate the existing image with a digital signature. The associated data in fact is termed as Global Data Frame. This data involves representative samples of one component or more of the color scheme of the image besides some other information regarding PC handler system and the capturing

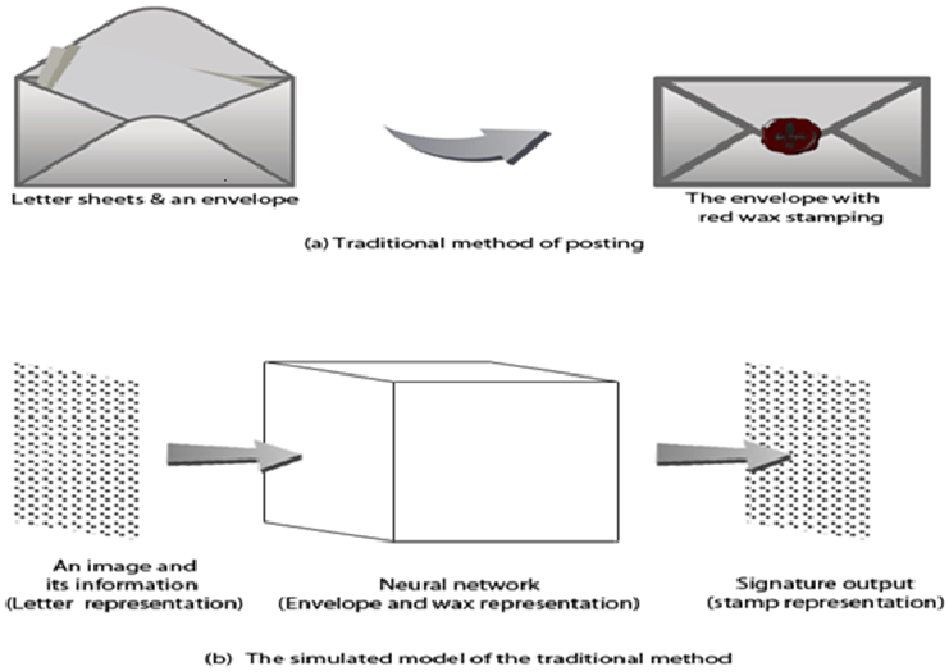

Figure 2. The overall simulation process of image association method of image protection.

instrument as scanner or camera or any other tool used for this purpose. Furthermore, to declare other views of information like atmosphere, capturing date and other personal information can be added.

The implementation processing involves two procedures; the first can be summarized by adding the information to the image in a wider frame environment; thereafter, sampling this frame into the same number of signature pixels using a key. Those samples of pixels are then reshaped to generate an array analogous to the dimensional distribution of the digital signature, that is, in same column and row sizes. The resulting array is considered as input patterns used to set a training table. The output of this table is organized with the digital signature itself. This procedure stands for watermarking imbedding procedure. Hence, a neural network is used to associate the given input with the required output of the digital signature and after training the structural attributes of the neural network are saved as a second key that is to be used along the second procedure along with the first key that is used for the sampling purpose.

In the second procedure, the image under verification is taken and appended with the claimed information to be fed to the sampling stage with the first key. The output of such sampled data is then applied as input to the second key which denotes the structure of the neural net to extract the output. This output is supposed to be the digital signature. When the signature emerges without any noise, it is considered as a great evidence for the ownership. But when this output is gathered with noise then verification fail for the ownership as evidence.

The conceptual foregoing attributes are translated via the programming modelling of the presented system. An image is appended with its related information representing many factors such as the location, time, camera model date, etc; and a neural network is used to tag this information with a selected signature of the owner. Any modification to the image would result in a disturbance of signature output. This neural unit is supported as a ready toolbox in Matlab; therefore it is of less concern over the design prospective. It is worth mentioning that one of the major obstacles that appeared is the dimension problems of data size. Programming facilities takes long time to manipulate pixel items of the image in the different stages of the association process, particularly speaking in neural network training. For this reason, the work substitutes the whole structure with definite samples. This is achieved by using a random number generator that is functionally implemented as coordinate sampler. A definite numbers of pixels and data is then fixed for the generation limits. The initial seed of the generation is usually referred to as a first key to embed higher level of security besides its original function of data dimension reduction.

Association procedure

This procedure is developed throughout the following four stages:

i) First stage: This stage is responsible for reading the original image and getting the header data of the image; writing this information in Excel file as vertical vector and producing and saving the file.
ii) Second stage: This stage is responsible for reading the original image with its size (rows and columns) and an Excel file (totalq.xls). Then it calculates the number of columns in original image with the size of rows. Then it makes a choice to increase a number of rows in the original image or not in order to fill incomplete size of row by zeros and to produce global data array by new Mat file.
iii) Third stage (watermark.m): This stage is responsible for reading the signature image as (Computer.bmp) and make (signature) as bitmap either (0 or 255) in two dimensions array, then save the array in file.
iv) Fourth stage (gen_inpout.m): This stage is the most important activity driven in the first procedure. Based on the dimension of the signature, a number of coordinates pairs are generated randomly. In this generation, a seed is set and considered as a first key used

later for the extraction procedure. For the generated coordinates, pixels are collected from the image and its information. Hence, three components are gathered and averaged to give a scalar value. When these data are evaluated, they are organized to create a pseudo image structure of two dimensions. Then, the essential requirements for the main function of this stage are prepared. The main function denotes a training phase of a neural network. Input/output association depends on the pseudo image as input and the signature as output. This organization allows for column wise pattern association, that is, each column from the input is correlated with a column in the output. General description of this stage is summarized by feeding the image and its information in addition to the first key (seed=123456). On the other side, this stage produces a neural structure as a second key, signature results of this association and finally the pseudo image.

Signature extraction procedure

In the second procedure there is just one program which is termed. This program reads the input after being reformulated in the style presented in the fourth stage of the previous procedure. In the course of this experiment, different inputs are used to complete the normal execution of the current stage; an example is this input. In addition to this input, this program needs the neural structure as well. When these materials are fed, the neural network is driven in the simulation mode of execution to generate the related signature.

The whole procedure ends up with a matching activity. The generated signature is compared with the original signature given with similar dimension. Matching output is posted when a ratio of 80% is recorded. Otherwise, mismatch signal is alerted for false signature announcing for illegal copyright. The matching activity is carried out by subtracting the generated signature from the original one. Non zero bits are collected and divided by the number of all dark pixels of the original signature. Hence, the matching ratio can be given by the following formula:

$$Mr. = \frac{(1 - Di)}{T} \times 100\ \%$$

Where Mr. is matching ratio, Di is the irregular pixel numbers that resulted from subtracting the generated signature from the original one, and T is the total number of zero pixels found in the original signature.

The decision of the matching is then given in accordance to the following conditions:

Yes; if Mr. > = 80%
No, if otherwise.

TESTING EXPERIMENTS

The first is investigated as an experiment of the association by feeding the image and appending its information. Then by using a Neural Network toolbox utility, the association is made to correlate global image, representing the image and its information from one side and owner signature from the other side. In this experiment a private key is used. This key denotes random number generation seed. When the related function is executed, a sequence of image coordinates is generated successively. Each coordinate represents a pair of row and column parameters. A set of coordinates can be adjusted by the application suiting the execution performance. High number will result in long time execution and little number will be faster. Hence the first key would be used to determine the initial seed required to evaluate the sequence generated to scan image samples. On completion of this experiment, a second key is generated. This key technically represents a multi valued factor that sums up the whole connection scheme of the neural network used for the association process. Undoubtedly, the association as a term is an interpretation of neural network learning procedure that needs a training table. This table is figured out here in this work as the global image and the signature declaring the input and output respectively. Parameter settings of the conducted experiment used the following values:

First Key: 123457

Inputs: Test_image.jpg as a training input; Jordan.bmp as a training output; Image size of test_image.jpg is pixels (each is 3 bytes); Image size of Computer.bmp is 44*96 pixels (each is 1 byte, with each pixel either 255 or 0 in value to give black and white scheme). Instead of manipulating bit wise, byte processing is carried out.

Outputs: Key 2; despite using the neural network connection structure (matrix) besides Key 1 as an input to the procedure, it is considered as output information needed for the protection scheme as essential materials of the management that should be kept at the owner sid training parameters (MatLab Neural Network Tool); no. of layers: Training error = 0.01.

In this experiment, neural structure impact is studied; where different number of neurons is used to test the performance of the association. Beginning with 10 neurons, our experiments showed that 60 neurons and more are suitable for our proposed model.

Robustness characteristic performance testing experiment

This set of experiments explains the validity measurements of the presented system. For robustness in watermarking techniques, image is supposed to be highly resistant to any distortion (intentional or unintentional) of data. Therefore, this test is conducted to make the image intentionally be subjected to a resizing process. This process is accomplished by size increase and decrease with different amounts and by specified algorithm. The implemented algorithms used are NEAREST, BILINEAR and BICUBIC. Output is viewed as a result of applying the change of the size and then recovering the original size again. In this, it is assumed that the used algorithm for the size changing is possible to be detected and applied once again to recover the

original size. Taking into consideration that these results could be further extended to involve the application of variant algorithm to any one of them, the work actually summarizes this experimentation process by applying the same algorithm used in size changing to eliminate the results as far as possible and to figure out the problem in brief cases.

Unlike the watermarking principles, the current work adopts a different strategy in recommending the matter of robustness resistance. Here the resizing is considered as illegal data activity and the system is supposed to be sensitive for any change in original data. Therefore, the following results show these contradictions of judgment towards this activity, in which, the signature when being generated with noise will indicate data hacking or illegal intruding. This capability is sought important to keep the original image unchanged. To discuss the experiments, original size of the image is referred to by X. And based on this assumption, the following experiments can be investigated.

Resizing with "NEAREST" algorithm

Dimension increasing mode

Using NEAREST algorithm, the original image dimension is increased with different factors, Resizing with 2(2*x) factor to Resizing with 6(6*x) factor.

With this algorithm of resizing, results show that the system successfully recovers the signature but at the same time it was not sensitive enough to indicate the activity of image resizing.

Dimension decreasing mode

Using NEAREST algorithm, the original image dimension is decreased with different factors: Resizing with 2 (2/x) factor to Resizing with 6 (6/x) factor.

The results show that the system could have the ability to detect the resizing activity carried on the original image.

Resizing with “BILINEAR" algorithm

Dimension increasing mode

Using BILINEAR algorithm, original image dimension is increased with different factors: Resizing with 2(2*x) factor to Resizing with 6(6*x) factor. The results show that the system could have the ability to indicate the resizing activity.

Dimension decreasing mode

Using BILINEAR algorithm, original image dimension is decreased with different factors: Resizing with 2 (2/x) factor to Resizing with 6 (6/x) factor. The results show that the system was able to detect the resizing activity.

Resizing with “BICUBIC" algorithm

Dimension increasing mode

Using BICUBIC algorithm, original image dimension is increased with different factors: Resizing with 2(2*x) factor to Resizing with 6(6*x) factor.

The result shows that the signature could be noticed; it could be deduced that the detection is accomplished successfully.

Dimension decreasing mode

Using BICUBIC algorithm, original image dimension is decreased with different factors: Resizing with 2 (2/x) factors to Resizing with 6 (6/x) factors.

The results show that, high detection is generated depending on the noisy output of the signature.

Illegal attack testing experiment

This experiment set denotes the functional application view that conjugates watermarking as a main reference. Watermarking despite the used techniques and methodologies when applied will result in a modification of the content of the original image. In this experiment random data injection is intentionally embedded with different ratios of 15, 25, and 35% as low rates simulating watermarking effect in modifying image content. The method of data modification is conducted by generating random pixel coordinates of row and column. For each pixel, random colour intensity is again generated. The amount of pixels is made equal to the required ratio of modification and as a function of the global amounts of image pixels.

The output of the three levels of data modifications shows apparently that the system is capable to detect the hacking processes.

Conclusions

This work proposes a protection system that is used for digital images. System design is based on the emerged contradictions between early application of watermarking and its recent implementation of protection. Main objective sought since the initiative time is to be aware of secret messages over a cover data such as images. However, recent implementation has directed the attention towards the image by subjecting the watermark as copyright evidence. Such matter motivates the initial work to seek for traditional strategies used for justice

investigations regarding properties ownership problems in addition to crime mining.

Logically watermark can be considered as evidence that is used for approving the copyright. But unfortunately when such evidence is attacked and removed, the protection planning as a whole would be failed. Hence, as much as there are more evidences, the matter of protection would be more secured. More evidences are difficult to be denied than using just one. On this wisdom the whole work of this research is established, that is, increasing the evidences of the owner.

Therefore the current work is thought to be integrating those two issues; original features and ownership evidences at the same time.

Evidences can be classified to fall into two different sorts. These sorts are personal and environmental factors. Personal sort involves all the parameters that detail the existing relations with the information of the person, such as family attributes, social and psychological parameters. Whereas, the environmental sort encompasses all the information related to timing and positioning factors. This might be clearer when adopting crime investigations. Obviously, evidences might be detected on victims with the aid of some materials that stick on the bodies. That means evidence is not necessarily implied with the victims but accompanied with. That is also true with the protection system under investigation in the current work. One can argue why it is necessary to imply the signature as evidence in the image as a watermark. Is it possible to associate this evidence with the image? In fact, the work gives suitable responses to these problems. It depends on the personal data and environmental information as integrated evidences that extend a signature item. It widened the area of justice to inrush many aspects rather than one especially when one or more evidences are denied. And finally, this system is capable to protect the original features besides its subject.

On application, results approved the validity of the successful model that is capable to involve all the referred features invoked earlier. Different schemes of neurons are tested and the most suitable scheme is decided. Besides, many other tests are all enrolled to show the performance estimations required to convince the application strategy.

REFERENCES

Abdallah Saleem Nawaf Al-Tahan Al-Nu'aimi, Rami Qahwaji (2009). Green Channel Watermarking to Overcome the Problem of Multiple Claims of Ownership for Digital Coloured Images. International Conference on Cyber Worlds, UK. pp. 339-344.

Aditya V, Rajarathnam N, Sanjoy P (2010).” NoMark: A Novel Method for Copyright Protection of Digital VideosWithout Embedding Data”, IEEE International Symposium on Multimedia.

Ali A, Ahmad M (2010). "Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition". Eur. J. Sci. Res. 39(1): 6-21.

Charlie O, Behzad S (2009). “DIGICOP: A Copyright Protection Algorithm for Digital Images”, TIC-STH.

Cox IJ, Miller ML, Linnartz JMG, Kalker T (1999). “A Review of Watermarking Principles and Practices” in Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, New York, Marcel Dekker, Inc. pp. 461-482.

Hsiang-Cheh H (2008). “Copyright Protection with EXIF Metadata and Error Control Codes”, International Conference on Security Technology.

Kutter MF, Hartung (1999). “Introduction to Watermarking Techniques”, in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, pp. 97-119.

Mei J, Li S, Tan X (2009). “A Digital Watermarking Algorithm Based On DCT and DWT”, Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA’09), Nanchang, P. R. China May 22-24, pp. 104-107, ISBN 978-952-5726-00-8.

Mn-Ta L, Shih-Syong C (2010). “Image Copyright Protection Scheme Using Sobel Technology and Genetic Algorithm “,International Symposium on Computer, Communication, Control and Automation.

Rongen PMJ, Maes MJ, van Overveld KW(1999). Digital image watermarking by salient point modification: practical results. In: Proceedings of SPIE Security and Watermarking of Multimedia Contents, 3657:273-282.

Tao B, Dickinson B (1997). "Adaptive, “Watermarking in DCT Domain", Proc. Of IEEE International Conf. on Acoustics, Speech and Signal Processing, ICASSP-97, 4:1985-2988.

Tilki JF, Beex A (1996). Encoding a hidden digital signature using psychoacoustic masking. Proceedings of the 7th International Conference on Signal Processing Applications and Technology, 476-480.