The Effect of Watermark Embedding on Signature Generation in Image Association Technique of Copyright Protection System

Mamoun Suleiman Al Rababaa
Computer Science Department, Information Technology Faculty,
Al al-Bayt University, Jordan

ABSTRACT
The current research enhances the performance of an already proposed image protection system presented earlier. The former system relies on an association technique instead of embedding owner signature inside an image like traditional watermarking methods. Thus, it retains secured image characteristics against any type of tampering two additional units are involved at the second phase of the former system operation. The main functions of those two units are to resize and reform the image as a preprocessing before submitting it to common processing of signature generation. Neural network structures are used to build those two units. A method of data compression is used to save time and generalization feature of neural network. Samples of pixels with their encoded coordinates are used to construct a data base used for the training purpose where the relative coordinate is used instead of the absolute address of the pixels and then encoded to determine a useful data suitable for neural network processing. Major conclusion remarks are discussed to highlight the most significant recommendations needed for future work.

General Terms
watermarkong, Security.

Keywords
Watermarking, Copyright, Digital Signature.

1. INTRODUCTION
Among the different methods of Image copyright protection, watermarking comes out as one of the techniques used to secure digital images [2] [3]. Functionally, watermarking is an extension of the steganographic early methods. Steganography uses different kinds of data like images or sometimes texts as a cover to hide inside important secret messages. Therefore, they are not of a great deal. Obviously, the cover letter, in this application, is no more than a media holding significant information, which is the secret letter, capable to deceive intruders and prevent them from approaching what is hidden inside.

The applications of image protection afterwards turned to use this technique in an alternative way. The cover has gained the interests over the secret message that represents a signature of an owner or a trade mark of a producer. Trends of image protection nowadays are focused to keep the cover as safe as possible without any change or corruption regardless it holds irrelevant foreign data. Nevertheless, watermarking continues using this method as a main approach in image copyright protection [4]. Accordingly, a digital product is kept protected as long as its accompanying owner signature kept inside unreachable by tampering attempts. However, watermarking looks for a difficult swinging resolution between changing cover data and keeping it unchanged. Embedding a signature is an intentional change of image data and on the contrary meeting the conditions of satisfying watermarking characteristics is a controversial goal to keep this data unchanged [5].

Technically, signature embedding principle causes major conflict between watermarking as a technique and its requirements. Embedding a signature into a letter requires many conditions to meet. These characteristics are partially met in certain adjustment but in another they don't.

They have never been thoroughly satisfied as they oppose each other. In fact, the presented proposal considers these characteristics as discordant and conflicting when it comes to gather them all simultaneously. At the time when watermarking tends to change the cover letter for embedding a signature, it strongly reject this change avoiding corruption to the same cover letter. Therefore, it is hard to keep the balance between the desire and the pragmatic facts of watermarking characteristics.

Based on these conflicts, a previous work presented a new technique for image copyright protection. This technique associates a data unit, which is an image and its related information, with a signature throughout a neural network structure. It is designed to preserve both specifications of size and color intensity of an original image without any modifications. In this technique, original image is considered as the main part rather than the embedded signature to qualify resisting any possible changes or modification during common processing or image transformation. As a complementary work to the presented new technique, the current proposal primarily tends to find out the effect of traditional watermarks on the second procedure of its model termed as signature generation. Thus, it is an attempt to expand ownership with reasonable judgments that are based on rigid results on signature generation. The work also tends to present an adequate procedure design to predict the type of any resizing algorithm used to transform an image from its original size to another size. Defining the effects and implementing the resizing algorithm as a supplementary tool to the proposed technique all together will allow further enhancements to efficiently secure the copyright of digital images.

The work is oriented to study the effects of different types of watermarking methods; spatial and transformational. It will also apply some image file formats. To generalize the embedding data, a spectrum of data density rates will be used to test the generated output. Each rate stands for a watermark shape and/or a style. A rate of pixel density is usually determined by the ratio of a selected number of pixels to the size of the image itself. In each rate sample, the values of a

corresponding number of image pixels will be changed randomly. The random change accounts for a method that generalize watermarking technique that will simulates an assumed arbitrary watermark color intensity values. A considerable range between 10% and 30% are used throughout the conducted experiments.

An algorithm predicting procedure can be designed with the help of another neural network structure. Identical network structure is assigned in each resizing algorithm. In this proposal three different algorithms are selected; Nearest, Bilinear and Bicubic. An original image and a resized copy of this image will be used as training patterns. Patterns are intended to involve a group of images which in turn comprise either pure images or embedded images of different watermarks and different resizing ratios as input and a unique output of the original image. Each combination of an image group with its unique output will be assigned to one network only. The training result of each net is thus supposed to determine an algorithm type in terms of the connection weighting of the concerned net. To decide which algorithm is used in any given resized image, this resized image sample will be fed to all the networks. The most accurate output will then highlight the related type of the resizing algorithm. Although the output is envisaged to not be totally perfect, it will definitely specify the type of the algorithm.

2. WATERMARKING REVIE

There are two main approaches used in watermarking. Both of them act to modify the multimedia cover according to embedding watermarks. 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 et.al. [6] 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 [7] 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 original watermark. Another example of spatial watermark algorithm is developed by Rongen et.al. [8]. It incorporates the use of the salient pixels for embedding the watermark. Their approach for watermark is shown to robust to rotation, scale, and translation. Besides it has proved resistance 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 behavior 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.

Al-Haj and Mohammad [9] 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 [10] 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 [11] 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 Jiansheng et. al.[12] 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 into as high frequency band into discrete wavelet. The reported algorithm results were invisible with good robustness for some multimedia processing operations.

A general focus on the main performance of the two approaches considered above can be featured out with the aid of adopting an example comparison between spatial and frequency domains that is depicted in table 1.

Table (1) comparison between spatial and frequency domains

Characteristic	Spatial Domain	Frequency Domain
Computation Cost	Low	High
Robustness	Fragile	More Robust
Perceptual Quality	High Control	Low Control
Capacity	High (depend on the size of the image)	Low
Example of Applications	Mainly Authentication	Copy Rights

3. WATRMARKING CHARACTERISTICS AND REQUIREMENTS

Watermarking mechanisms can be characterized by a number of requirements which are sought by any proposed application [5]. 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. As it is mentioned previously, the presented model suggests the association principle in order to avoid the results carried out from injecting or modifying data. The main expected requirements for watermarking works can be summarized as below:

(1) Perceptibility: the watermark image should be indistinguishable from the original cover image, i.e. watermark should not distort or affect the cover image [1], and thus it will be undetectable or unnoticeable except by the owner.

(2) 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 .

(3) Integrity: No loss of original multimedia carrier.

(4) 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.

(5) Compatibility: watermarked multimedia data should keep certain level of compatibility with the original data.

and unintentional when the image is resized or rotated. In both cases image data will no longer be unchanged.

The trends of upgrading the new technique extends the fundamental presented procedures by two more additional functions, Fig 1. The first is to set up the original state of image orientation and dimension while the second is to retrieve the lost data resulting from tampering the original

(6) Traceability: Watermarking can be repeated along a processing line in order to accommodate for multiple watermarks that reflects the stage throughout a tracking process.

Security: watermarking accounts for the protection of ownership against forgery and unlawful threats.

4. THE ENHANCED PROTECTION SYSTEM

The new technique applies its copyright protection by a strategy of combining image evidence with its content, and then associating the resultant data with owner's signature. Unlike traditional procedures of watermarking , this technique doesn't embed a signature inside image content but it associates it with the image along with its related evidence externally using a neural network. There are two security keys which are used to secure owner's product. A random seed integer, which is the first key, reduces the dimension of the data prepared for the association activity while selecting data from the image and its related evidence. Whereas, a neural network structure, which represents the second key, is used to extract owner signature from the data scanned from the image by the first key. However, system design involve two different stages of signature associating and signature extracting. The first stage generates the two keys when it runs identifying the required structure of the associating neural network. Owners have to keep those two keys safely as main issue of their properties. And when dispute occurs the second stage grants the signature of the owner to approve the copyright by executing the related procedures of signature extraction. In the early presentation of the this technique, there was no awareness to consider essential mediating procedures that are supposed to recover any corrupted data resulting from exterior tampering attempts onto the secured image. The current work is focused on this investigation where it highlights the possible tampering effects. They are usually either intentional or unintentional. Intentional when embedding fake signatures into the secured image takes place

image . These two functions altogether complete the required activities in the second stage to extract signatures. The first function resizes and aligns the image to fit the exact dimension and alignment of the secured original image. Then after, the output of this function moves to the second function of data retrieval before reaching the last activity of the procedure. The second function uses another neural network structure to retrieve, as much as possible, the lost data before extracting the signature.

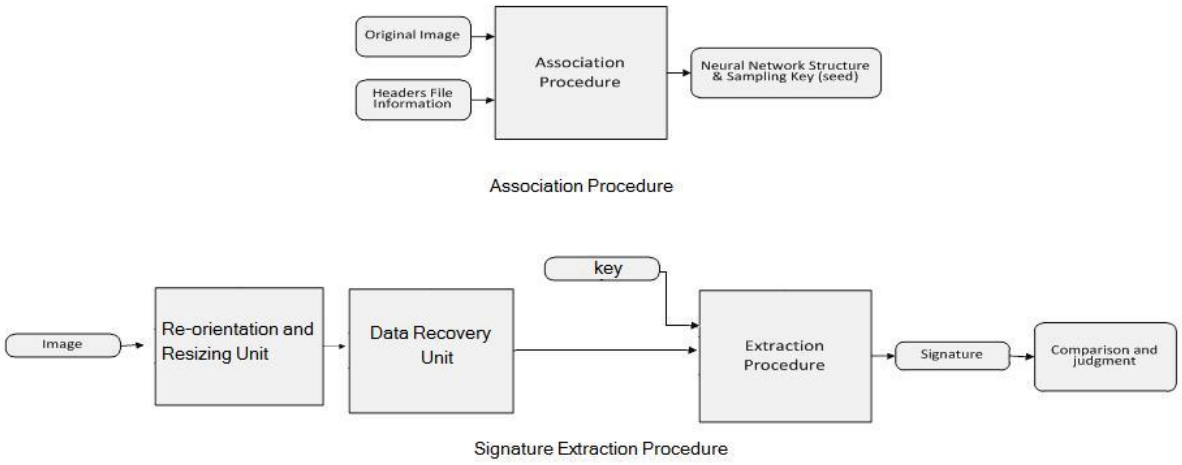


Fig.1 The Enhanced Protection System

Training the new neural network uses a set of corrupted images as input and the original image as output. Image copies with different noise distribution are adequate training samples to cover wide variations. When input dimension is large, neural network needs a long execution time to train. Therefore, four different data recovery sub units are designed. Each of which undertakes one quarter of the in question image. Noise is intentionally created on the original image at each quarter and a proportion data samples are selected for the recovery process. The most important consideration is given to the way samples are collected. At each coordinate, a sample of data is registered. This coordinate then after is expanded into a set of relative digit representation. Coordinates are represented by a decimal coded digits in order to highly discriminating data items in the input of the training set. The more digits used, the more distinctions results. Each digit value, as required by neural networks, ranges between 0 and 1. The scoring is a relative measure computed from dividing the given coordinates by the size of the image and then scored as a fractional value in each decimal digit. As an example, coordinates of 30, 60 on an image size 319 X 118 pixels, can be represented using 6 or more decimal digits. The relative measures in terms of 6 neural input digits, as an example, can be computed in two steps. The first is to find the relative coordinates :

relative row index: 30/319 = 0.094, and

relative column index : 60/118 = 0.508

, and the second is to find the final digit scores by dividing each digit of the decimal score by 9:

row index = 0/9 9/9 4/9 = 0 1 0.44

columns index = 5/9 0/9 8/9= 0.55 0 0.88

In result, the decimal digits summing up this representation are as follows:

0 1 .44 .55 0 .88 , noting that the first are reserved to row index whereas the last three digits are to the column index.

These coordinates besides image data are the elements of the training input. Any difference detected from the comparison will turn to a record comprises image data and related coordinate digits. Fig. 2 clarifies this manipulation of data to give the final table of the training with a single color and three color component images.

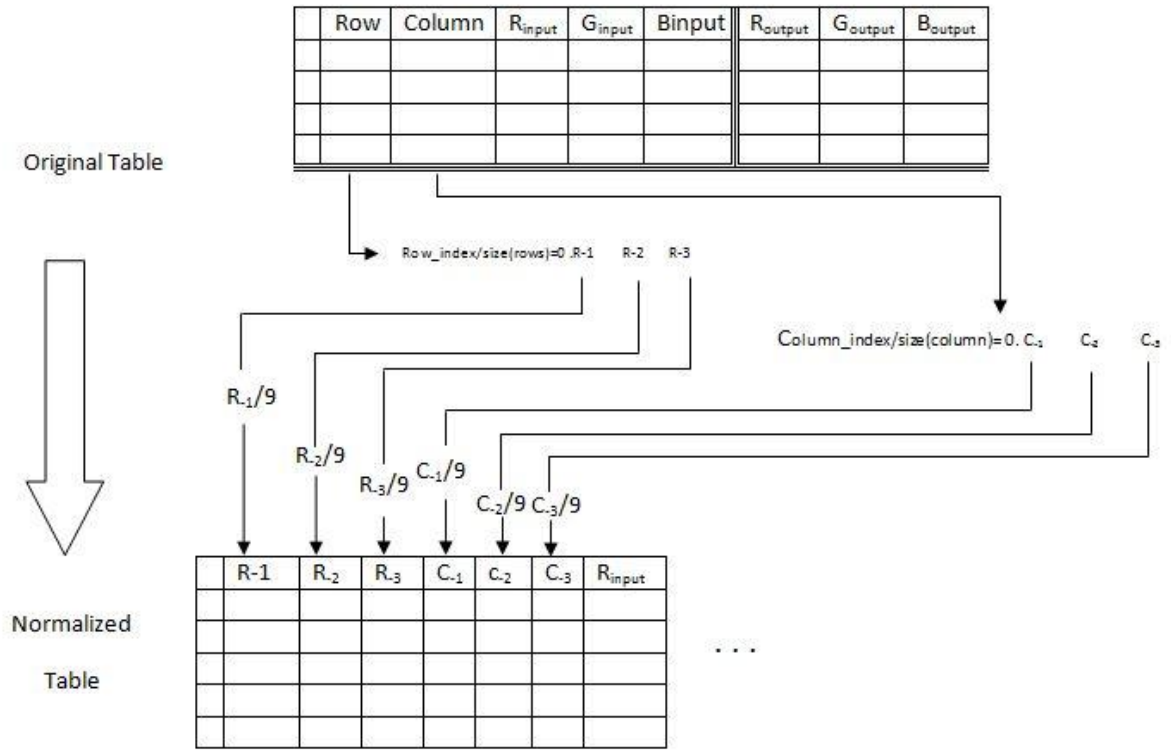
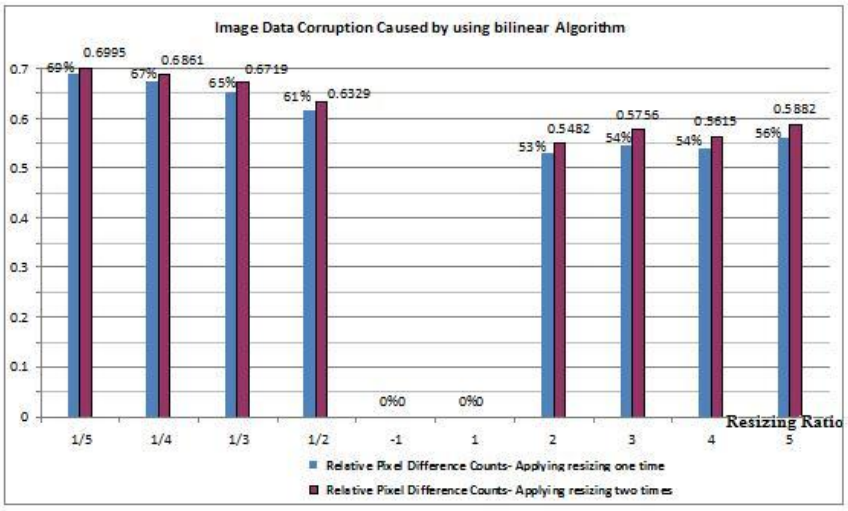
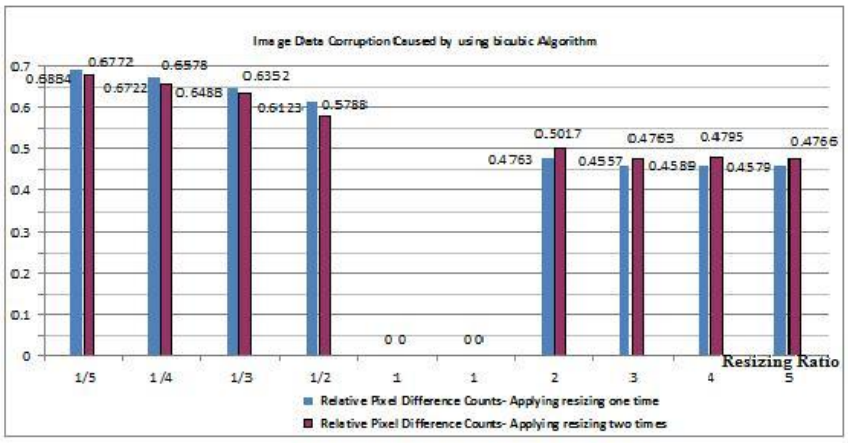


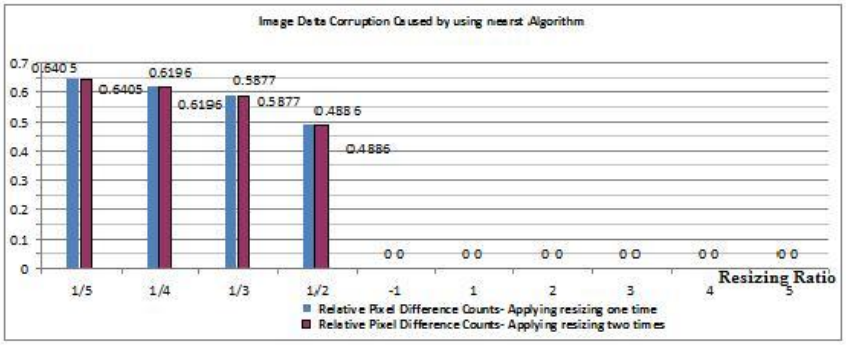
Fig 2. Address Decimal Normalization

4.1 Resizing Stage

For this activity, the received alleged image can be simply recovering its orientation and size by using common processing as required by comparing it with the original copy of the image. With this activity, it is therefore an image is expected to hold the corrupted data result from embedding fake signature of alleged owners and/or all the processes acts to resize or put the image in new orientation. Fig. 3 shows different impact of applying resizing algorithms on an image. From this figure it can be easy to clarify how corruption is varied when different algorithms are used. Three different algorithm are studied in this work. Each style has its own feature that distinguishes it from the other two. They are namely Nearest, Bilinear and Bicubic. Despite the algorithm used to resize the original image, the second process of data recovery is capable to resolve this corruption.







Resizing Impact on Digital Images

4.2 Data Recovery Stage

As mentioned earlier, four different sub units are designed to recover data corruption loss. Each of which is built by a neural network . Training is done by creating noise and embed it into the original image with different ratios. Training table is organized to comprise an input of a a corrupted data on one hand and original content of the image on the other hand. Noise is graded with different ratio randomly on the image. Images in return are considered as a random samples and for each one four recovery quarter net are set out. Results have been investigated in terms of direct study and indirect. Direct in terms of the counts of the recovered pixels and indirect in terms of its impact on signature association. The results are summarized by two figures in Fig. 4 and Fig 5 respectively. Obviously the corresponding signature associating procedures are quite satisfactory with respect to the noise compensation results depicted in Fig 5.

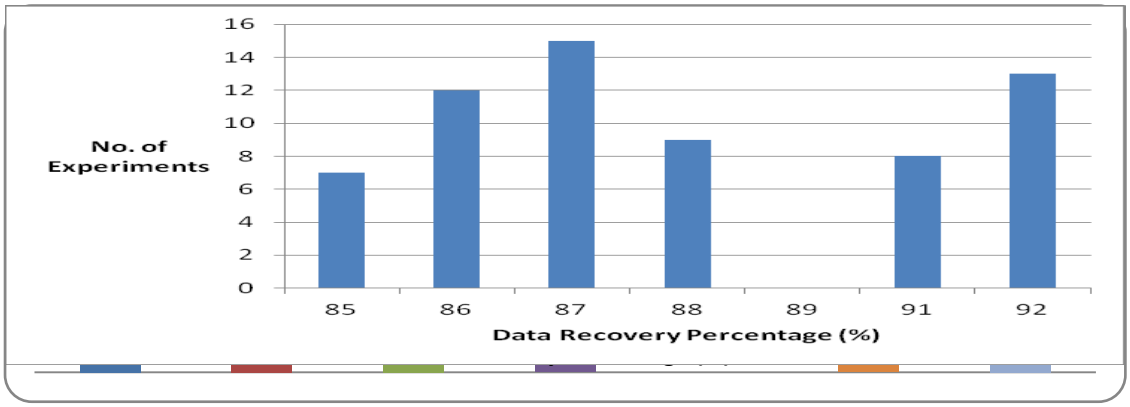


Fig. 4 Direct Data Recovery Summary

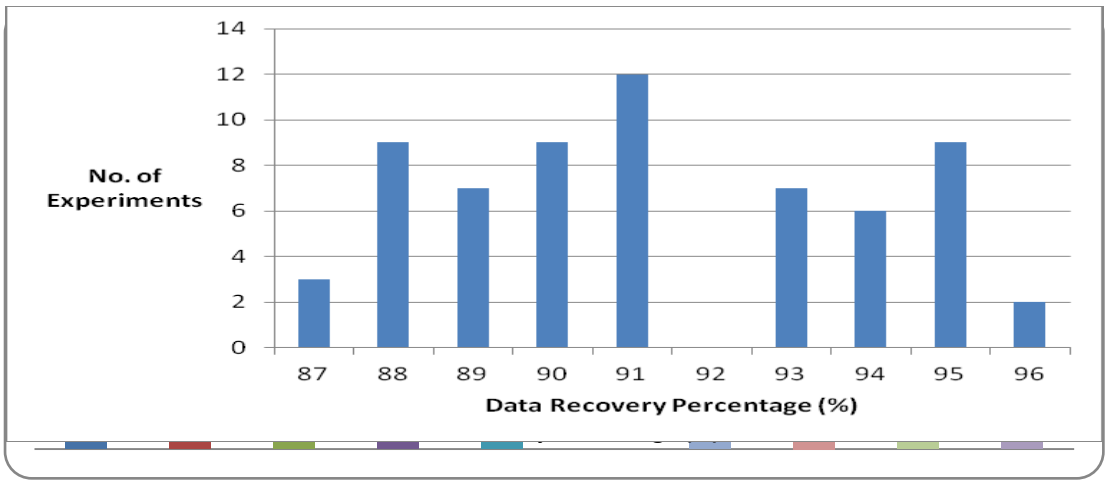


Fig 5. Indirect (signature) Data Recovery Summary

5. CONCLUSIONS

This work enhances a previous image protection system that implements a new strategy of associating signature with an image instead of embedding it. Additional two processes are included to resolve for tampering attempts of illegal ownership. These two processes return original size and orientation of any tampered image by recovering its corrupted data as much as possible. For resizing, common algorithms have been used whereas for the data recovery four different neural networks are used. Each neural net is assigned to one quarter of the image to extend number of pixel variation. The training tables are made sensitive to the coordinates of pixel covered. the linear address is normalized in terms of three digits referenced to max decimal value.

The work studied the effect of resizing impact on images as a step towards healing such effect. In this study, resizing is made by increasing or decreasing the size and then turning it back to the original size. Within such process image pixel difference are registered to show the relevant impact in question. On the other hand the work go further to obtain the resolve proposed for the recovery of data corrupt. Based on the results obtained, it is found that the enhancements added by those two processes is quite efficient and satisfactory. The overall presented system with the enhancements made has been examined in wide range of experiments and it has been strongly convincing to be adopted as a successful tool for image copyright protection that retain all the features required for the protection such as size, orientation and content.

REFERENCES

[1] Hsiang-Cheh Huang and etal., "Copyright Protection with EXIF Metadata and Error Control Codes", International Conference on Security Technology, 2008.

[2] Aditya Vashistha, Rajarathnam Nallusamy, and Sanjoy Paul," NoMark: A Novel Method for Copyright Protection of Digital Videos Without Embedding Data", IEEE International Symposium on Multimedia 2010.

[3] Mn-Ta Lee and Shih-Syong Chen, "Image Copyright Protection Scheme Using Sobel Technology and Genetic Algorithm "International Symposium on Computer, Communication, Control and Automation2010.

[4] Charlie Obimbo and Behzad Salami, "DIGICOP: A Copyright Protection Algorithm for Digital Images", TIC-STH 2009.

[5] Cox I.J., M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and Practices" in Digital Signal Processing for Multimedia Systems, Ed, K. K. Parhi, T. Nishitani, New York, Marcel Dekker, Inc., 1999, pp 461-482.

[6] M. Kutter, F. Hartung, "Introduction to Watermarking Techniques", in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 97-119.

[7] Abdallah Saleem Nawaf Al-Tahan Al-Nu'aimi and Rami Qahwaji, "Green Channel Watermarking to Overcome the Problem of Multiple Claims of Ownership for Digital Coloured Images", 2009 International Conference on CyberWorlds, International Conference on CyberWorlds, 7-11 Sep., 2009, Bradford, UK , PP339-344, ISBN: 978-0-7695-3791-7. DOI 10.1109/CW.2009.60

[8] Rongen, P.M.J., Maes, M.J., van Overveld, K.W.: Digital image watermarking by salient point modification: practical results. In: Proceedings of SPIE Security and Watermarking of Multimedia Contents, vol. 3657, pp. 273-282 (1999).

[9] Ali Al-Haj and Ahmad Mohammad, "Digital Audio Watermarking Based on the Discrete Wavelets Transform and Singular Value Decomposition", European Journal of Scientific Research, Vol.39 No.1 (2010), pp.6-21, ISSN 1450-216X, http://www.eurojournals.com/ejsr.htm

[10] 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.

[11] Tao B. and Dickinson B., "Adaptive, "Watermarking in DCT Domain", Proc. Of IEEE International Conf. on Acoustics, Speech and Signal Processing, ICASSP-97, Vol.4, pp.1985-2988, 1997.

[12] Mei Jiansheng, Li Sukang and Tan Xiaomei, "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, 2009, pp. 104-107, ISBN 978-952-5726-00-8.