

Securing Digital Images Integrity using Artificial Neural Networks

Tarik HAJJI, Zakaria ITAHRIOUAN & Mohammed OUZZANI JAMIL

Laboratoire Systèmes et Environnements Durables (LSED), Faculté des Sciences de l'Ingénieur (FSI), Université Privée de Fès (UPF) , Fez, Morocco

hajji@upf.ac.ma

Abstract. Digital image signature is a technique used to protect the image integrity. The application of this technique can serve several areas of imaging applied to smart cities. The objective of this work is to propose two methods to protect digital image integrity. We present a description of two approaches using artificial neural networks (ANN) to digitally sign an image. The first one is “Direct Signature without learning” and the second is “Direct Signature with learning”. This paper presents the theory of proposed approaches and an experimental study to test their effectiveness.

1. Introduction

Watermarking Is a technique to add copyright information or other verification information to a file audio, video, image or any other document. The message added to initial information, usually called brand, is a set of bits whose content depends on the application. The brand can be the name or identifier of the creator, owner, buyer or a form of signature that describes the host signal [1].

Artificial Neural Networks (ANN) is a problem resolution mechanism, inspired by the human brain reasoning. The ANN basic unit is the artificial neuron. An ANN is made up of a neurons collections organized in layers: The first layer the input layer, the last is the output layer and the layers in the middle are called the hidden layers 1 (Figure 1).

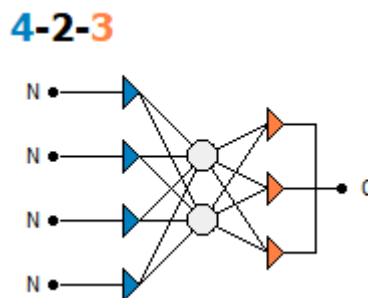


Figure 1. Artificial Neural Networks

An ANN is characterized by a specific architecture to define its neural structure. In this work we propose a notation to define this architecture, for example the notation **ANN (64, 16, 64)** indicates the use of a multilayer ANN compound by:

- An input layer composed by 64 artificial neurons,
- One hidden layer composed by 16 artificial neurons,
- An output layer composed by 64 artificial neurons.

We distinguish two ways of using ANN:

- Use with learning: We have a database composed by a partial solution of the problem. Then, we use an algorithm to teach ANN the resolving mechanism of the different instances of the

problem. The gradient back propagation is a famous algorithm able to comprehend an ANN the comprehension mechanisms. Finally, we can use the ANN after learning to solve new instances of the problem.

- Use without learning: In some cases, we have no information about the solution space for the problem studied. For example, the problem of classification which we do not have classes to classify elements. So we can use an ANN in unsupervised mode to find the classes firstly (clustering).

This paper presents in the first part some performed researches in the area of digital image signature. The second part contains the methodology used to sign digital images presented by our approach. The last part is dedicated to results presentation and discussion.

2. Digital signature

2.1. State of the art

Before developing our approach of digital image signature, we started by identifying research work in the same field. Baltzakis & al. presents a new online system of signature recognition and verification. The proposed system is based on texture features. In the first step, the classifier combines the decision results between the neural network and the Euclidean distance obtained by using the three sets of features. The results of the classifier of the first stage are used as input of the function of the second step (radial base structure of the ANN) which makes the final decision. The entire system has been extensively tested and resulted in a strong recognition and verification rate [2].

Sabourin & al. propose an ANN approach to build the first stage of an automatic system of handwritten signature verification. The directional probability density function was used as an overall form factor and power of discrimination has been strengthened by reducing its cardinal by filtering. Different experimental protocols were used to implement the ANN. As a comparison, on the same database and the same decision rule, we show that the BPN classifier is significantly better than the classifier threshold and it is compared favourably with the classifier k-nearest neighbour [3].

Yin Ooi & al. propose the hybrid methods of discrete Radon transform, principal component analysis, and probabilistic ANN. The proposed framework is designed to distinguish genuine signatures counterfeit depending on the image level. They realised experiments on their own database and on the MYCT database. Equal error rate (EER) of 1.51%, 3.23% and 13.07% are reported, respectively, for false random, casual and skilled in their own database. By working on the basis of MCYT signatures, their proposed approach strikes an AIR of 9.87% with 10 training samples [4].

2.2. signature verifiers

The objective of signature verification is to prove authenticity of the image form a regular basis. The signature verification techniques used are divided into two categories: online (dynamic) and offline (static).

The online approach uses a compressed tablet produced by digital compression to extract information about the signature and takes dynamic information such as compression speed, writing speed, number of stroke order and pen pressure at each point [5]. The application fields of this technique include the protection of the computers, the permission of computer users to access sensitive data or programs and people authentication for access to physical devices or buildings [6].

The offline approach involves less electronic control and uses signature images captured by camera or scanner [7]. An offline signature verification system uses features extracted from the digitized signature image. The characteristics used for online signature verification are simple and invariant [5]. therefore, the only pixel image must be estimated. However, the offline systems are difficult to design, because many of the characteristics are recognized immediately [6].

3. Methodology

3.1. Direct signature without learning

We started our work by simply using ANN to sign a digital image. Two ANN was used without learning: (64, 4) and (64, 16, 4). After a random initialization of ANN synapses, we generated the signature mark of the image.

The signature brand that we have generated is a square matrix of 64 * 64 of real numbers. Figure 6 shows a sample of this matrix which is constructed recursively as follows:

- Creating sub block size of 64 pixels.

- Propagating each block in the ANN and retrieving in the output another block of 4 pixels.
- Reconstitution of the blocks generated by the ANN to form a new image.
- If the image is smaller strictly to $2 * (64 * 64)$, then our brand signature is the first block of size $(64 * 64)$ retrieved from the image.
- If not, it returns to the first step and we repeated the treatment on the new matrix.

Table1. Example of signature brand matrix

0,3909787	0,5942461	0,1758067	0,570799
0,7838546	0,4328258	0,9424887	0,134017
0,6287956	0,0495958	0,9381059	0,295321
0,8730479	0,6471385	0,7373837	0,33285
0,9164182	0,1429214	0,1170479	0,388731
0,9753208	0,997113	0,2675925	0,2199
0,7721224	0,9261069	0,126968	0,465133
0,3155098	0,3050952	0,8643453	0,404389
0,3844193	0,8711779	0,2627959	0,420844
0,4696244	0,3227052	0,4210994	0,937877
0,7938168	0,2988817	0,6899086	0,672164
0,0246497	0,3149587	0,3639539	0,711749
0,8075495	0,7368181	0,4869043	0,321361

3.2. Direct signature with learning

We used the ANN (64,16,4) with an unsupervised learning algorithm deduced from the back-propagation of the gradient [8].

Learning principle is based on our concept of image and signatures similarity rate that we have defined in the introduction of this work.

We built the training base by slightly modified images of Lenna (1000 copies). Figure 2 shows an example of these images.

**Figure 2.** Example images of the learning database

The similarity rate of these two images is very elevated ($T(M1, M2) = 0.001$), we evaluate the degree of similarity of the signatures produced by the two images.

The objective of learning is to ensure a higher level of divergence between signatures. Our ultimate goal is to have two completely different signatures for two infinitely similar images so we can prove the strength of our solution against attacks. The learning algorithm is as follow:

1. Random Initialization of weight.
2. Propagation of signal presented on ANN inputs.
3. Propagation of signal in to the hidden layers.
4. Propagation of signal to the output layer.
5. From the second iteration of the algorithm, we calculate the rate of similarity between the current image (the block: SC) and the previous image (the block: ST).
6. If $ST > SC$ then we go directly to the next image (block).
7. If not we go to step 6.

8. Back propagation of error.
9. Updates of knowledge in the weight.
10. Loop to step 2

The graph 3 represents the convergence of learning depending on the iteration number.

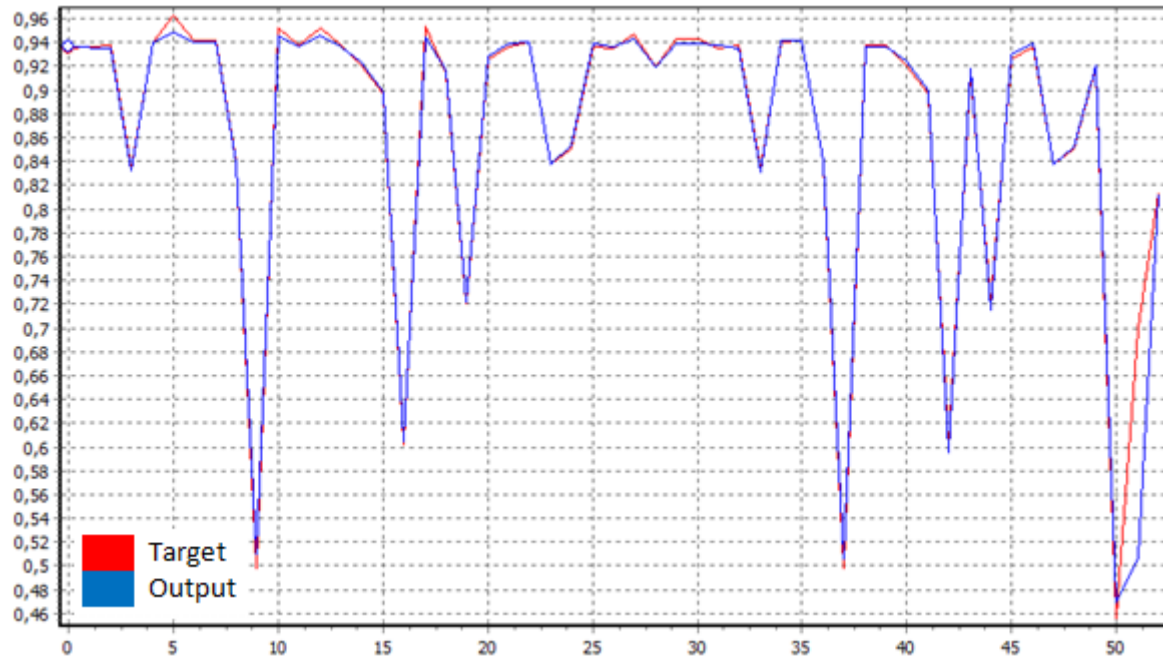


Figure 3. Convergence of learning based on iterations number

4. Results & Discussion

4.1. Direct signature without learning

The desired results are to prove experimentally the relationship between the image and signature similarity rate with the direct signature. Table 2 shows an excerpt from results:

Table 2. Excerpt from results of direct signature without learning

Image and signature similarity rate		Image m1	Image m2	Image m3	Image m4	Image m5	Image m6	Image m7
		T(m1, mi)	T(m2, mi)	T(m3, mi)	T(m4, mi)	T(m5, mi)	T(m6, mi)	T(m7, mi)
Image m1	T(m1, mi)=0.001	1	0,791633	0,180129	0,073344	0,552294	0,839633	0,333491
Image m2	T(m2, mi)=0.002	0.001	1	0,085628	0,502186	0,523391	0,998496	0,988435
Image m3	T(m3, mi)=0.003	0.002	0.001	1	0,87703	0,641848	0,208981	0,949327
Image m4	T(m4, mi)=0.004	0.003	0.002	0.001	1	0,269716	0,608958	0,687738
Image m5	T(m5, mi)=0.005	0.004	0.003	0.002	0.001	1	0,839663	0,421186
Image m6	T(m6, mi)=0.006	0.005	0.004	0.003	0.002	0.001	1	0,358951
Image m7	T(m7, mi)=0.007	0.006	0.005	0.004	0.003	0.002	0.001	1
	Image similarity rate	S(m1, mi)	S(m2, mi)	S(m3, mi)	S(m4, mi)	S(m5, mi)	S(m6, mi)	S(m7, mi)
	Signature similarity rate							

Images and signatures similarity rate with $0 < i < 1025$

This table is composed of 1,000 Lena images infinitely close. The red boxes represent the similarities rate between two images and the blue boxes to represent the signatures similarities rates for both images.

The graph of Figure 4 shows the relationship between the similarity rate of the images and signatures to our database composed of 1,000 of infinitely close.

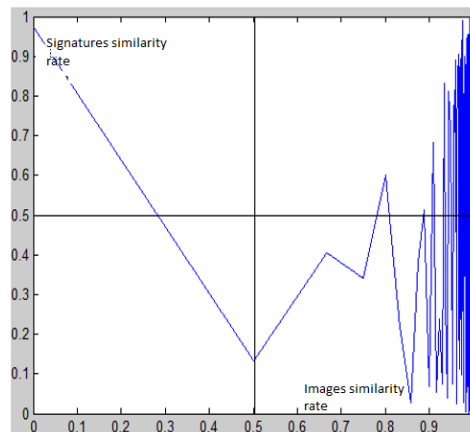


Figure 4. Relationship between the similarity rate of images and signatures (without learning)

Note that this graph is not 100% random, which proves that we have a partial relationship between the similarity rate of the images and signatures. This reflected a major drawback to the approach without learning. Because we can calculate the signature trademark of an image if we have the signature of another relatively close image.

To solve this problem, we used unsupervised learning for multilayer ANN.

4.2. Direct Signature with learning

Table 4 shows a second excerpt of the matrix of calculated results with ANN (64,16,4) with the unsupervised learning algorithm.

Table 3. Excerpt from results of direct signature with learning

Image and signature similarity rate		Image m1	Image m2	Image m3	Image m4	Image m5	Image m6	Image m7
		T(m1, mi)	T(m2, mi)	T(m3, mi)	T(m4, mi)	T(m5, mi)	T(m6, mi)	T(m7, mi)
Image m1	T(m1, mi)=0.001	1	0,791633	0,180129	0,073344	0,552294	0,839633	0,333491
Image m2	T(m2, mi)=0.002	0.001	1	0,085628	0,502186	0,523391	0,998496	0,988435
Image m3	T(m3, mi)=0.003	0.002	0.001	1	0,87703	0,641848	0,208981	0,949327
Image m4	T(m4, mi)=0.004	0.003	0.002	0.001	1	0,269716	0,608958	0,687738
Image m5	T(m5, mi)=0.005	0.004	0.003	0.002	0.001	1	0,839663	0,421186
Image m6	T(m6, mi)=0.006	0.005	0.004	0.003	0.002	0.001	1	0,358951
Image m7	T(m7, mi)=0.007	0.006	0.005	0.004	0.003	0.002	0.001	1
Image similarity rate		S(m1, mi)	S(m2, mi)	S(m3, mi)	S(m4, mi)	S(m5, mi)	S(m6, mi)	S(m7, mi)
Signature similarity rate		Images and signatures similarity rate with $0 < i < 1025$						

Figure 5 shows the relationship between the similarity rate of the images and signatures for images we studied.

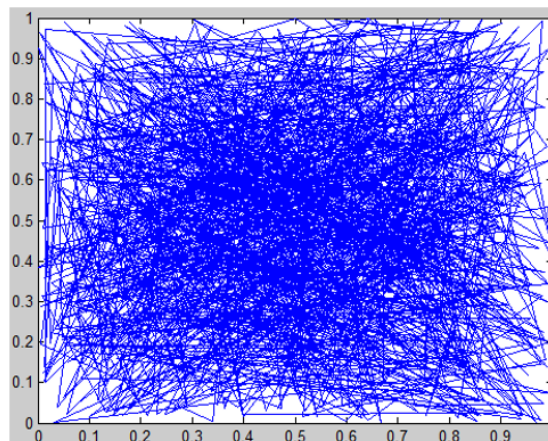


Figure 5. Relationship between the similarity rate of images and signatures (with learning)

The graph in figure 5 is completely random. We can conclude that this approach cannot provide the same signature for both images regardless of their degree of similarity.

5. Conclusion

We have presented in this work, contributions that use ANN in different ways to protect the image integrity. We found that with unsupervised learning, we cannot have two identical signatures for two images, whatever their degree of resemblance. This new approach is very important because for two almost identical images, one can check which one is original and which one is falsified.

Our approach has several advantages:

- It offers both a reliable signature and verification method.
- It is independent of any signature or verification key.
- It is independent of the form of the signed image.
- The size of the signature is the same and does not depend on the image size.
- It is resistant to various attacks.

However, the main inconvenience of this approach is the difficulty of the use of ANN especially the relatively large learning time.

References

- [1] F. Cayre, C. Fontaine, & T. Furon, « Watermarking security: theory and practice », IEEE Trans. Signal Process., vol. 53, no 10, p. 3976- 3987, 2005.
- [2] H. Baltzakis & N. Papamarkos, « A new signature verification technique based on a two-stage neural network classifier », Eng. Appl. Artif. Intell. vol. 14, no 1, p. 95- 103, 2001.
- [3] J.-P. Drouhard, R. Sabourin, & M. Godbout, « A neural network approach to off-line signature verification using directional PDF », Pattern Recognit., vol. 29, no 3, p. 415- 424, 1996.
- [4] S. Y. Ooi, A. B. J. Teoh, Y. H. Pang, et B. Y. Hiew, « Image-based handwritten signature verification using hybrid methods of discrete radon transform, principal component analysis and probabilistic neural network », Appl. Soft Comput., vol. 40, p. 274- 282, 2016.
- [5] O. C. Abikoye, M. A. Mabayoje, & R. Ajibade, « Offline signature recognition & verification using neural network », Int. J. Comput. Appl., vol. 35, no 2, p. 44- 51, 2011.
- [6] M. V. Pandey & S. Shantaiya, « Signature verification using morphological features based on artificial neural network », Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, no 7, 2012.
- [7] P. Shikha & S. Shailja, « Neural network based offline signature recognition and verification system », Res. J. Eng. Sci. ISSN, vol. 2278, p. 9472, 2013.
- [8] K. Ben & P. Van der Smagt, « An introduction to neural networks », Univ. Amst., 1996.