Blind Fake Image detection

Nidhal El Abbadi[1], Adil Mohamad Hassan[2], Mudher Mohammed AL-Nwany[3]
[1]Computer Science Dep., University of Kufa
Najaf, Iraq

[2]Mathematical Dep., University of Kufa
Najaf. Iraq

[3]Mathematical Dep., University of Kufa
Najaf. Iraq

Abstract
With the great convenience of computer graphics and digital imaging, it becomes much easier to alter the content of images than before without any visually traces to catch these manipulations. Many fake images are produced whose content is feigned. Thus, the images cannot be judged whether they are real or not visually. In order to detect fake images, this paper proposes a blind detection uses singular value decomposition (SVD) as a classifier to make a binary decision on whether an image is fake or real. This work is an improvements process to an existence method to detect fake image using SVD. The experimental results prove the effectiveness of this algorithm to detect any small changes in image even with one dot of real image.

Key words: *SVD, fake image, singular value decomposition, image processing.*

1. Introduction

Cameras are regarded as trustworthy devices and photos traditionally imply truth. Nowadays, digital photos have been widely used as historical records and as evidences of real happenings in applications from journalist reporting, police investigation, law enforcement, insurance, medical and dental examination, military, and museum to consumer photography.
While digital photos are conveniently used, their credibility has been severely challenged due to numerous fraudulent cases involving image forgeries, e.g. the fake results on human stem-cell research [5].

With the availability of powerful image editing tools, numerous image retouching techniques have become practical, which can be used to create great artistic works.

However, malicious modification of image content forms a serious threat to the secure and legal usage of digital images.
By skillful manipulation, forgery may be very difficult to recognize by the naked eye. Therefore, automatic detection of image forgery has attracted much research interest. In recent years, many image forgery detection techniques have been proposed, especially passive approaches which do not require any additional information besides the image itself [5] [6].
Some published methods make use of lighting abnormality [1], blur moment invariants, and similarity/dissimilarity of color and structural characteristics [3].
Digital tools have enabled easy image creation, modification and distribution, which make fraudulent image forgeries easier than ever.
Fakes are created either by merging two or more photos or altering an existing image. Because image manipulation happens at the pixel level, detection is not as easy as it was before the digital era. Tricky fakes can be exposed by algorithms that detect discrepancies or statistical irregularities at the bit level.
An image is authentic if it represents a witness to an actual event, place, or time.
A definition of image authenticity should enable us to distinguish an authentic image from the fake images, such as the 2D composite images and the 3D computer graphics images.
It is still a problem how to detect whether digital images are fake or real. Generally, there is an obvious boundary between the fake area and the real area, with the improvement of desktop photograph manipulation software, which cannot be used to distinguish fake images and real images. There are a many studies related to detect the fake images. In [5], a blind detection of photomontage is introduced using higher order statistics, where photomontage is a

similar concept with image fakery. In [6], a model based on bipolar signal perturbation is introduced to detect spliced images. These two papers used a statistics model and bi-coherence features to detect image forgery, and they are often used to detect human speech signal. In [1], Popescu and Farid introduced some techniques of exposing digital forgeries by detecting traces of resampling, which also tried to resolve the similar problem. Mahdian and Saic [2] used periodicity due to interpolation to perform blind image authentication. They introduced Radon transform on the basis of second derivative to detect rotation without estimation of the rotation angle.
In this paper, a SVD based fake image detection scheme is developed, which uses the change of the direction of the eigenvector in orthogonal subspace to detect the evidence of image fakery.

2. Singular Value Decomposition

In linear algebra, the **singular value decomposition** (**SVD**) is a factorization of a real or complex matrix, with many useful applications in signal processing and statistics.

SVD is based on a theorem from linear algebra which says that a rectangular matrix *A* can be broken down into the product of three matrices - an orthogonal matrix *U*, a diagonal matrix *S*, and the transpose of an orthogonal matrix *V* . The theorem is usually presented something like this:

$A_{m\times n} = U_{m\times m}.\, S_{m\times n}.\, V^T_{n\times n}$ 1

2.1 **Proposition:**

If $A = USV^T$ and

$v' = v + \alpha v_1 \frac{\|v\|}{\|v_1\|}$, $A' = US'V^T$,

then $A = A'$ when $\alpha \to 0$.

Proof:

$$\lim_{\alpha\to 0} v' = \lim_{\alpha\to 0} (v + \alpha v_1 \frac{\|v\|}{\|v_1\|}) = v$$

Then $v' = v$ when $\alpha \to 0$ $S = S'$

And this implies to $A = A'$

since [$A = USV^T$ *and* $A' = US'V^T$]

2.2 **Theorem:**

$\frac{\|v-v'\|\ \|v_1+v_2\|}{\|v'\|\ \|v_1\|} = \sqrt{2} * \frac{\|v-v'\|}{\|v'\|}$, and it's unique.

Proof:

$\frac{\|v_1+v_2\|}{\|v_1\|} = \frac{\sqrt{2}*\|v_1\|}{\|v_1\|} = \sqrt{2}$ (since v_1 and v_2 are orthonormal),

Then $\frac{\|v-v'\|\ \|v_1+v_2\|}{\|v'\|\ \|v_1\|} = \sqrt{2} * \frac{\|v-v'\|}{\|v'\|}$

To prove it's unique

Since v is unique (**as properties of *SVD***),

And v' is unique (since $v' = v + \alpha v_1 \frac{\|v\|}{\|v_1\|}$)

So $\sqrt{2} * \frac{\|v-v'\|}{\|v'\|}$ is unique.

2.3 **Corollary:**

$\frac{\|v-v'\|\ \|v_1+v_2\|}{\|v'\|\ \|v_1\|} \to 0$ when $\alpha \to 0$.

Proof:

By theorem 2.2 we have

$$\frac{\|v-v'\|\ \|v_1+v_2\|}{\|v'\|\ \|v_1\|} = \sqrt{2} * \frac{\|v-v'\|}{\|v'\|}$$

Then when $\alpha \to 0$ we have

$\|v-v'\| \to 0$

$\therefore \sqrt{2} * \frac{\|v-v'\|}{\|v'\|} \to 0$

$\therefore \frac{\|v-v'\|\ \|v_1+v_2\|}{\|v'\|\ \|v_1\|} \to 0$ when $\alpha \to 0$.

2.4 **Corollary:**

$A = B$ If and only if

$\sqrt{2} * \frac{\|v_A-v_A'\|}{\|v_A'\|} = \sqrt{2} * \frac{\|v_B-v_B'\|}{\|v_B'\|}$

Proof:

By theorem 2.2

$(\sqrt{2} * \frac{\|v_A - v_A'\|}{\|v_A'\|})$ is unique and,

$(\sqrt{2} \frac{\|v_B - v_B'\|}{\|v_B'\|})$ is unique,

$\therefore \sqrt{2} * \frac{\|v_A - v_A'\|}{\|v_A'\|} = \sqrt{2} * \frac{\|v_B - v_B'\|}{\|v_B'\|}$ If and only if $A = B$

3. Methodology

The proposed method to detect the fake image can achieve by processing image in many steps as follow:

1. First the original image A is transformed using SVD:

$$A = USV^T \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad 2$$

Where U and V are the orthogonal matrices, V^T denotes the transpose of V, and S is a diagonal matrix whose diagonal elements can form a column vector v.

2. Two secret column vectors v_1, and v_2 are constructed, which satisfy $|| v_1 \cdot v || = 0$, $|| v_2 \cdot v || = 0$, and $|| v_1 \cdot v_2 || = 0$

Where '$\cdot$' denotes the inner product.

3. The main goal is to protect the image before publishing it to the public; this will be achieved by changing the diagonal of S matrix result from relation (2) with new elements counted by the following equation:

$$v' = (v + \alpha v_1) \times \frac{|| v ||}{|| v_1 ||} \ldots\ldots\ldots 3$$

Where α is a scalar factor, which is set to 0.0001 for the purpose of this research.

The vector v' from relation (3) is restored as new diagonal elements into zero matrix S' correspondingly, for that new image will be constructed (A') as a protected image from the following relation:

$$A' = USV^T \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad 4$$

A' is the preprocessed image and publish to public.

SVD is robust to slight alteration of images, i.e., the vector v is stable under slight alteration of the image. In proposed image preprocessing procedure, the alteration of the vector v in relation (2) is very small, keep $v' \approx v$ **by Proposition 2.2** ,so the image preprocessing does not change the quality of origin image significantly (which will be demonstrated in the later examples).

4. Another suggestion in current research is using auto threshold (T_{th}) **by Theorem 2.3.** instead of constant threshold (0.01) for all images as in previous researches, which mean for each image there is specific threshold counted by the following relation:

$$\text{Threshold} = \sqrt{2} \times \frac{\|v - v'\|}{\|v\|} \quad \ldots\ldots\ldots 5$$

3.1 Fake Image Detection

When we have an image $A\hat{}$ and need to check whether it's fake or not, it will be decompose using SVD as follow:

$$A\hat{} = U\hat{}S\hat{}(V\hat{})^T \quad \ldots\ldots\ldots \quad 6$$

Then the vector $v\hat{}$ is extract from the diagonal elements of $S\hat{}$. The proposed fake image detection can be given as follow:

$$P = \left\| \frac{v\hat{}}{\|v\hat{}\|} . \frac{v_1}{\|v_1\|} \right\| + \left\| \frac{v\hat{}}{\|v\hat{}\|} . \frac{v_2}{\|v_2\|} \right\| \ldots\ldots 7$$

Where P is the detection value, which denotes the fake factor of the test image.

if $P > T_{th}$, then the tested image is fake, otherwise it isn't fake **by Corollary 2.5**, In the current proposed scheme, the two secret vectors, v_1 and v_2, are the key construction, on which the detection result depends.

We supposed

$\| v_1 \| = \| v_2 \|$ and $v\hat{} = v' + v_f$ $\ldots\ldots\ldots\ldots 8$

However, the vector $v\hat{}$ is composed of two vectors, one is the original vector v', and the other is the fake vector v_f.

Relation (7) can rewrite by using the equivalents' in relations (8) to get:

$$P = \left\| \frac{v' + v_f}{\|v\hat{}\|} . \frac{v_1}{\|v_1\|} \right\| + \left\| \frac{v' + v_f}{\|v\hat{}\|} . \frac{v_2}{\|v_2\|} \right\| \quad \ldots\ldots\ldots\ldots 9$$

Relation (9) can be computed approximately as follow:

$$P \approx \left\| \frac{v_f . (v_1 + v_2)}{\|v\hat{}\| \, \|v_2\|} \right\| = \frac{\|v_f\| \|v_1 + v_2\|}{\|v\hat{}\| \, \|v_2\|} = \sqrt{2} \, \frac{\|v_f\|}{\|v\hat{}\|} \quad \ldots\ldots 10$$

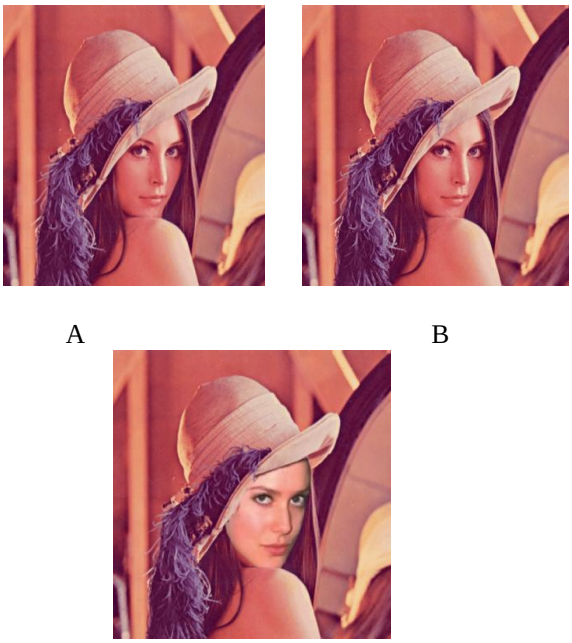
by Corollary2.4

It is obvious that the detection factor P depends on the fake vector v_f where $v_f = v' - v\hat{}$ and since $v', v\hat{}$ are unique (**properties of *SVD*)** so that v_f is unique, while v_f denotes the fake vector of the tested image, so the detection value P can reflect the status of fake image. Also, there are two secret vectors in our proposed process, v_1 and v_2, which do not have influence on the absolute value of detection result.

4. The result

To prove the proposed method we will take some of image and make intended change on it to see how this algorithm works.

4.1 The first image is the famous image (Lenna) as shown in fig 1, the origin image will protected by applying relations (3, and 4), it is clear the origin image have no perceptual difference from the protected image. Intended changing made on the protected image by changing the face of Lanna. The auto threshold for this image which is (1.3555e-004) counted by relation 5, also the fake factor counting using relation (10) which is equal (0.0185), it is clear ($P > T_{th}$), then the tested image (C) is fake.



A B C

Fig 1: (A) origin image. (B) Protected image (image 1). (C) Fake image

4.2 The second example is to test the effect of rotation on the result of this method. Protected image of Lenna (image B in fig 1) is rotated with 90 degree.

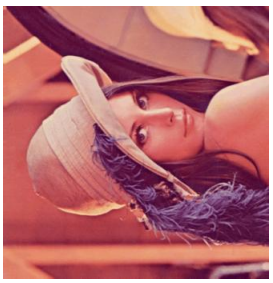
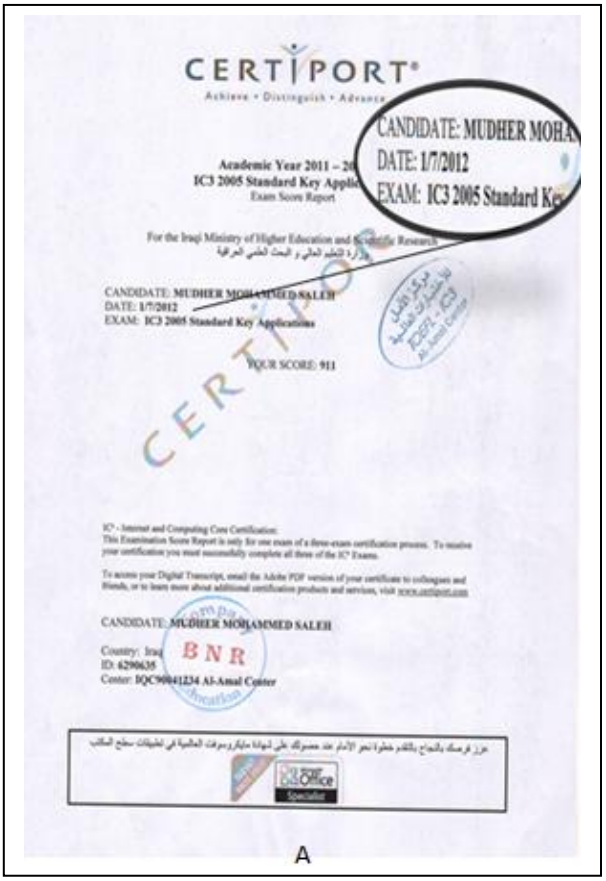


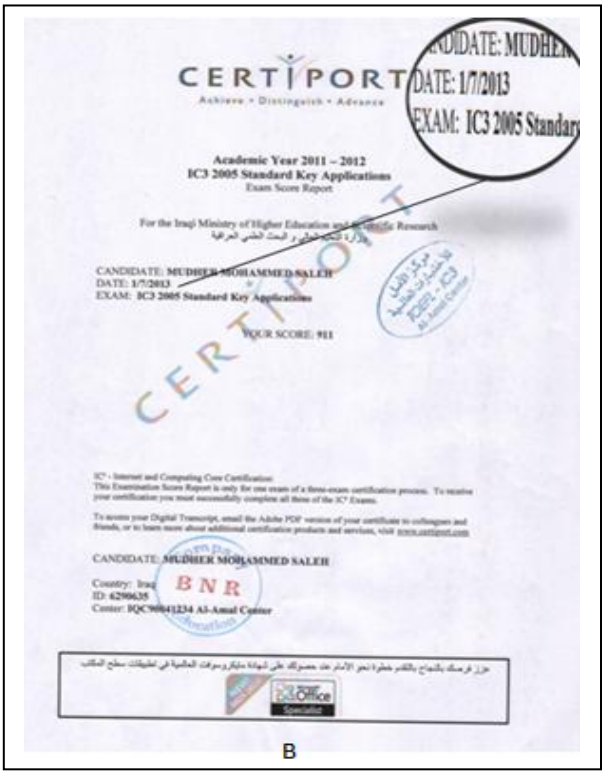
Figure 2: rotated image for test (image2)

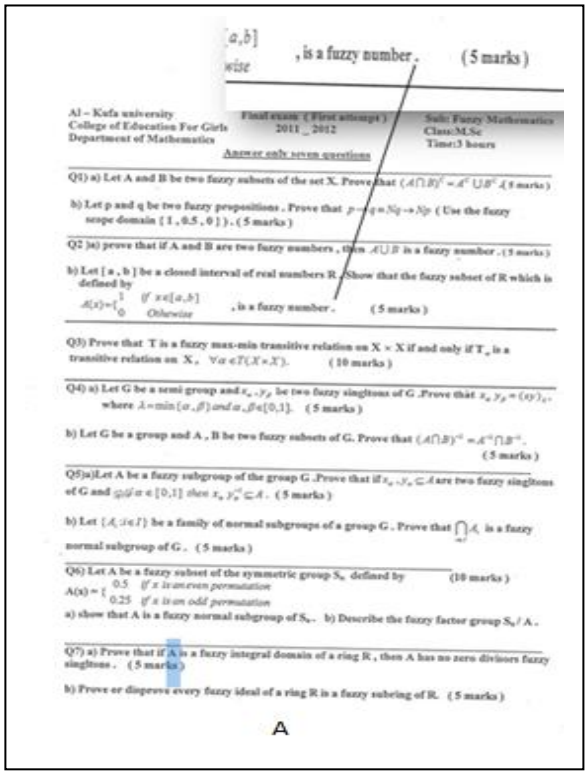
Then the counted fake factor P of image in fig 2 was (1.3462e-004), so we decided **by Corollary2.5.** this image is original ($P < T_{th}$).

4.3 Third example to test small change in copy of IC3 certificate, the change is made by changing one number only in the date (1/7/2012 change to 1/7/2013). Fig 3 shows the two IC3 images.



A





The P of this image (2.4055e-004) greater than threshold T_{th} of this image (1.0191e-004)**.** So it's fake **by Corollary2.5. .**

4.4 The fourth example done on the copy of questions (Fuzzy mathematics exam) which we change just one dot on it as shows in fig 4. The threshold of the protected image was (1.4142e-004) while the fake factor P = 1.9060e-004, which is greater than threshold of this image. So the image is fake **by Corollary2.5.**

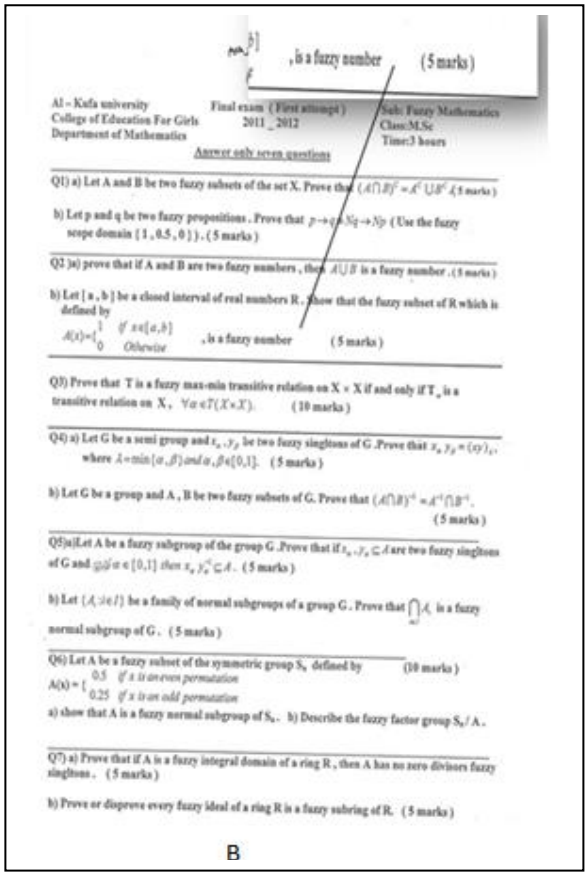


Fig 4: (A) the protected image (image 4). (B) Fake image.

4.5 To summarize the results from the above examples, and to prove the results, table 1 compares the results from the proposed method with the result by the paper of [7].

Table 1: Results of experiments compared with Lai Chung method [7].

Method	No. of image	1	2	3	4
Previous method	T_{th}	0.01			
	PSNR	Average = 38			
Proposed method	Fake factor (P)	0.0185	1.3462e-004	2.4055 e-004	1.9060 e-004
	T_{th}	1.3555e-004	1.3555e-004	1.0191 e-004	1.4142 e-004
	PSNR	107.0874	107.0874	91.3923	87.6442
	Decision	Fake	Origin	Fake	Fake
	Reality of Images	Fake	Origin	Fake	Fake

5. Conclusions

In this paper, we used SVD technique for fake image detection Scheme. Before the images are published to public, some assistant information is inserted into them. Recurring to the secret information, the work in [7] introduced the mathematical SVD operation in fake image.
In this paper a modification of pervious work especially in [7] is achieved.
We calculated the two secret vectors in new method.
The important improvement in this work is the scalar factor expanding from 0.01 to 0.0001.
Also there is another improvement related to threshold, where the threshold in [7] was constant for all images, while in this work the threshold will be different for each image, auto threshold determine for each image instead of constant threshold (0.01). These improvements enhance the detection efficiency and eliminate false detection, in [7] the false positive rate was 0.8% when checking 1000 image while in this paper the rate decreases to 0.0%.

We must note that all method of detect fake image need the original image and the fake image to make recognition between them but in current method the origin image no longer needed.
A comparison between previous work and this work is studied where the sample test taken as color images.
We can make a decision that our SVD scheme is very excellent in detecting fake image and it's sensitive for any small area modified in any image.

References

[1] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of resampling", IEEE Trans. Signal Process., vol.53, no.2, pp.758–767, Feb. 2005.

[2] B. Mahdian and S. Saic, "Blind authentication using periodic properties of interpolation", IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 529–538, Sep. 2008.

[3] Steve J. Leon; "Linear Algebra with Applications", Macmillan Publishing Company, New York; 1996.

[4] T. Konda, Y. Nakamura, "A new algorithm for singular allude composition and its parallelization", Parallel Comput. (2009), doi:10.1016/j.parco .2009.02.001

[5] T.T. Ng, S.F. Chang, and Q. Sun, "Blind detection of photomontage using higher order statistics", IEEE Int. Symp. Circuits Syst. (ISCAS), pp.688–691, May 2004.

[6] T.T. Ng and S.F. Chang, "A model for image splicing" ,IEEE Int. Conf. Image Process. (ICIP), pp.1169–1172, Oct. 2004.

[7] Wei LU, Fu-Lai Chung, *and* Hongtao LU, "Blind Fake Image Detection Scheme Using SVD", IEICE TRANS. COMMUN., VOL.E89–B, NO.5 2006.

Nidhal El Abbadi, received BSc in Chemical Engineering, MSc, and PhD in computer science, worked in industry and many universities, he is general secretary of colleges of computing and informatics society in Iraq, Member of Editorial board of Journal of Computing and Applications, reviewer for a number of international journals, has many published papers and three published books (Programming with Pascal, C++ from beginning to OOP, Data structures in simple language), his research interests are in image processing, biomedical, and steganography, He's Associate Professor in Computer Science in the University of Kufa – Najaf, IRAQ.

In 1963 born in Najaf city, Iraq .Has MSc in applied mathematics from university of Technology, Baghdad. Has PhD in fractal geometry. He is a viewer of scientific journals and conferences. Member of the ministerial committee for updating the career. Member of ministerial virtual learning committee. More than 25 papers were published in locally journals and conference.

He graduate from College of education department of mathematics from AL-Mustanseria University/ Baghdad 1994, Worked as a teacher of Mathematics in the secondary schools, currently MSc. student in university of Kufa, mathematical department.