Digital signature with Visual cryptography

Mini Agarwal

Assistant Professor in Computer Science Department, College of Engineering, Teerthanker Mahaveer University Moradabad (U.P.). E-Mail: miniagarwal21@gmail.com

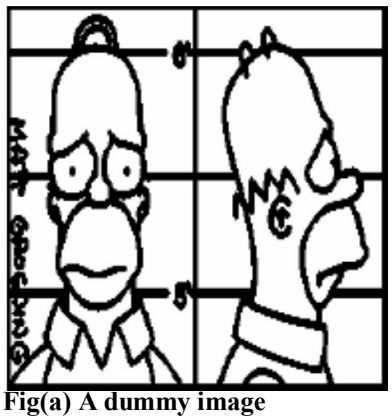
Abstract: We all know that digital signature is very good technology for stopping the hacking but it is a very lengthy procedure. For checking that the digital signature is authenticated or not than we have need to authentication software and for decrypting the signature we have need to private key and for encrypting the signature we have need to public key this is a very time consuming and money wasting method. So in this paper I combined the digital signature with visual cryptography. When I combined the digital signature with cryptography then we have no need to any authentication software or public and private keys. No one can hack these signatures because we splitting the signature in two pieces means in two sheets in black and white dots. So when we combined these two technologies then it's a very good method for stopping the hacking and it saves money. Only sender know that which sheet have a receiver so no one can generate the sender or receiver sheet means receiver is also not know that what is in his own sheet.

[Mini Agarwal . Digital signature with Visual cryptography**.** Journal of American Science 2011;7(9):861-863]. (ISSN: 1545-1003). http://www.americanscience.org.

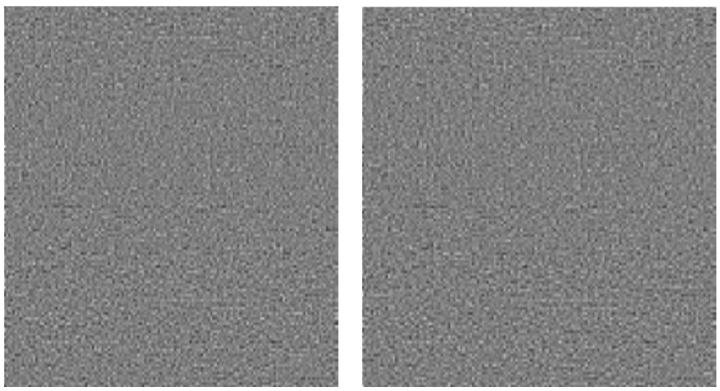
Keywords: hacking, money, splitting, white and black dots, technology.

1. Introduction:

Visual cryptography is a very good technique for stopping the hacking. According to the Naor and Shamir In this technology any picture, text any thing splits in to the two sheets in black and white dots. No one can check that this any important text or document these two sheets without together is a waste or rough sheets when we combined this two sheets then we get the important or useful text. So when we use digital signatures with digital cryptography then we splitting the digital signatures in to two sheets so in these two sheets we gave the any one sheet to the receivers and generate the second sheet that we attached with the message. When I combined the both sheets then this black and white dots make a full signature. When we combined these two sheets then we got the authenticated signature. So only sender is know that which sheet he sends to the receiver or he is the only person that makes the second sheets that he attached this with the email. In below fig (a) we have an image. In fig (b) we split the fig (a) in to two sheets in black and white pixels and fig(c) shows the combined picture after combining the both sheets. So fig (a), (b), and(c) show that how image or text or signature works in a visual cryptography.



Fig(a) A dummy image



Fig(b) splits the fig(a)

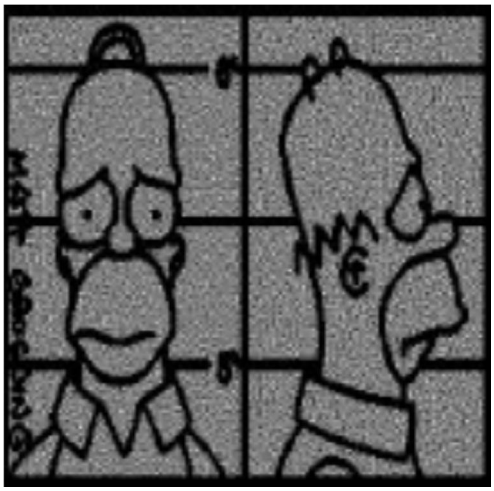


Fig (c): After combining the splits images

2. How Visual Cryptography works:

We all know that in visual cryptography images , text or signatures divides in to the black and white pixels. So these pixels are divided according to some rules means one white pixel and one black pixel. If two black pixel then two white pixel. The working phenomena are given below:

a) In the table (a) on the right we can see that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overplayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.[2]

b) We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.[2]

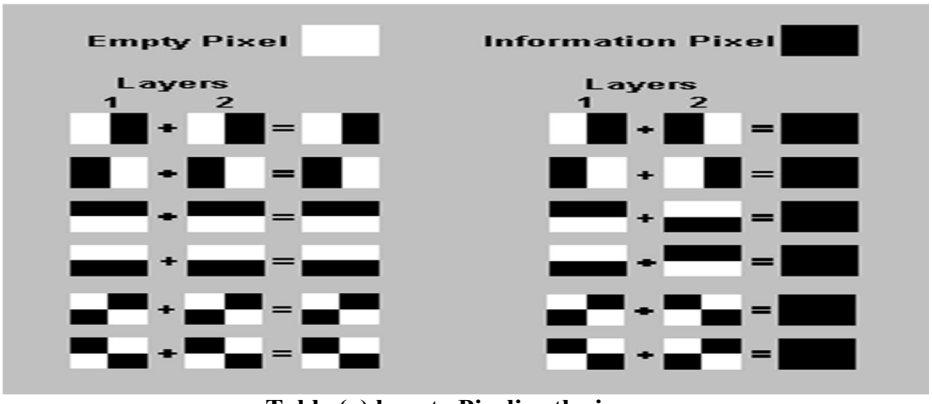


Table (a) how to Pixelize the image

3. Algorithm:

Naor and Shamir proposed the visual cryptography. I am merging this technique with digital signature technique. The algorithm is given below:

a) Pick up the signature.

b) We split the image in equal white and black pixels mean if we create 4 white pixels then we create same 4 black pixels.

c) One sheet sent to the receiver in advance.

d) Second sheet generated and send by the sender with the document or email. It is the

second sheet of first sheet that is send to the receiver.

e) Combined or merging the both splitting sheets.
f) Check both sheets make a complete signature or not.
g) If complete signature is found that means no one can did the changes in document.
h) If complete signature is not found that means one can did the changes in document.

4. Advantages:

a) Less time consuming than other cryptography techniques.
b) Provide confidentiality.
c) Provide authentication without any authentication software.
d) Only right receiver or sender knows about the encryption and decryption process.
e) Money saving.

5. Disadvantages:

a) Quality of image decreases after decryption.
b) Its technique is not user friendly.
c) If sender or receiver forgets their images then they cannot encrypt or decrypt the data or information.
d) It is a one-time pad system so if the image not splits in to right black and white pixel than it is not useful.

Conclusion:

Now I conclude my paper in this paper I am merging the two technologies visual cryptography and digital signature. I want to stopping the hacking because in digital signature one can hack the data or do the changes in the data if he know about the private and public key but in visual cryptography no one can hack the data because in this we are not using the keys in this we using the images with white and black pixel. Only sender knows about the image receiver is also no about the image receiver get the image when he combined both the image. Otherwise individual sheets are waste sheets.

References:

1) Fig(a) (b) (c) http://homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf
2) http://users.telenet.be/d.rijmenants/en/visualcrypto.htm
3) Table (a) http://users.telenet.be/d.rijmenants/en/visualcrypto.htm.

8/23/2011