A Survey on Digital Image Authentication

Ms. Mithra.K[1], Mrs. Nandhini. S[2]
[1]Dept of Computer Technology
[2]Assistant Professor, Dept of Computer Technology
[1, 2] Sri Krishna Arts and Science college, Coimbatore

Abstract- *Digital image is a numeric representation of 2D image which is composed of binary digits (0's and 1's). There are two types of images, they are vector image and raster image, it is identified by using the image resolution. Digital image refers to raster image. The term is commonly assumed to imply or embrace the process, compression, storage, printing, and show of such pictures [1]. A key advantage of a digital image is the ability to create copies with no loss of image quality. Digital transmission makes fabricating and replacing the image easier than ever before. Therefore, it demands systematic and automatic techniques to spot and verify the content of digital transmission [2]. Image authentication is one such method to mechanically identify whether or not the original image could be a fabrication or effortless copy of initial one.*

This paper aims at surveying various image authentication technique of digital image.

Keywords- Bitmap, hash function, watermarks, cryptography.

I. INTRODUCTION

An image is a visible impression obtained by a different device and displayed on a laptop or video screen. An image may be one that has been created or traced and kept in electronic form. A picture is represented in terms of vector graphics or formation graphics. A picture which is in formation kind is typically known as a bitmap. A picture map may be a file containing data that associates totally different locations on a given image with machine-readable text links [3]. Digital image authentication involves a scientific analysis which incorporates visible analysis and digital data analysis. The image authentication investigation does not stop within the digital world. In biological research, a loss in quality is scientifically ascertained and documented. This quality loss detection is additionally applied once digital image authentication is done using file formats like JPEG, BMP, TIFF, PDF .[4].

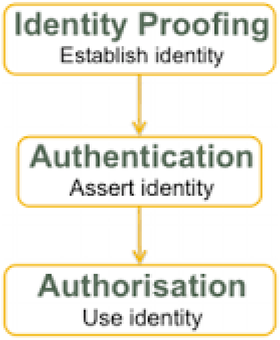

Fig 1 : Authentication Process

JPEGs are stored in the form of .jpg files [4]. Digital images are compressed using lossy compression. These images are captured by digital photography.

GIF file format supports image files up to 8 bits per pixel. This format uses lossless compression for compressing the image. GIF files frequently have the .gif extension along with the file name.

PNG is a file format for compression that was designed to supply a variety of enhancements over the GIF format. Like a GIF, a PNG file is compressed in lossless fashion (meaning all image data is rebuilt once the file is decompressed throughout viewing). We can store the image file in .png format.

SVG is Scalable Vector Graphics, which is used to define a graphical picture in XML format. Quantifiability means the file will be viewed on a CRT screen of any size. The display may a tiny screen of a smartphone or an outsized wide screen in a laptop. Sometimes we can store the image in .svg format.

TIFF (Tag Image File Format) might be a standard format for exchanging formation graphics (bitmap) photos between application programs. A TIFF file will be known as a file with a .tiff or ".tif" with end of file name [4].

II. IMAGE AUTHENTICATION REQUIREMENTS

- Sensitivity: The authentication process should be able to detect any content modification or manipulation. For any authentication algorithms, detection of manipulation is needed including content modification.
- Robustness: The authentication system should tolerate content conserving manipulations.
- Localization: The authentication system should be able to locate the image regions that are altered.
- Recovery: The authentication system should be able to partially or fully restore the image regions that were tampered.
- Security: The authentication system should have the capability to protect the authentication information against any falsification attempts.

III. DIFFERENT TECHNIQUES FOR IMAGE AUTHENTICATION

- Watermarking based authentication
- Cryptography based authentication
- Robust image hashing authentication

A. Watermarking Based Authentication

Digital watermarking is the art and science of embedding copyright information within the files; the data which are embedded in files are named as watermarks. Digital watermark is one which contains all the signals that are additionally added to a document to authenticate it and to prove the possession.

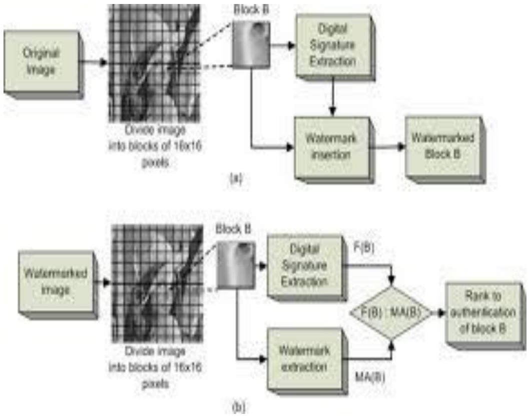
Original Image
Block B
Digital Signature Extraction
Divide image into blocks of 16x16 pixels
Watermark insertion
Watermarked Block B
(a)
Watermarked image
Block B
Digital Signature Extraction
F(B)
F(B) : MA(B)
Rank to authentication of block B
Watermark extraction
MA(B)
Divide image into blocks of 16x16 pixels
(b)

Fig 2: Watermarking Based Authentication

There are two types of watermarking approaches. They are

- fragile watermarking
- strong watermarking

Advantages:

- Implementation on the system platform is possible.
- Embedding watermarks is easy.
- Image tampering can be recognized.

Disadvantages:

- Does not prevent image copying.
- Watermark disappears if someone manipulates the image.
- Resizing and compressing the images from one file type to another file may decline the watermark and it becomes unreadable.

B. Cryptography Based Authentication

Cryptography is the study of exchanging the documents or pictures in secure communication. It includes two functions encoding and decoding. In cryptography algorithms, conventional cryptography show satisfying results for image authentication with high tamper detection. Localization performances do not seem to be superior but it is acceptable for a few applications. Even a little modification within the image pixels or perhaps in the binary image information causes changes as results of the hash operations are extremely sensitive. The image is assessed as manipulated, once only one little bit of this image is changed; this is often terribly severe for many of applications.

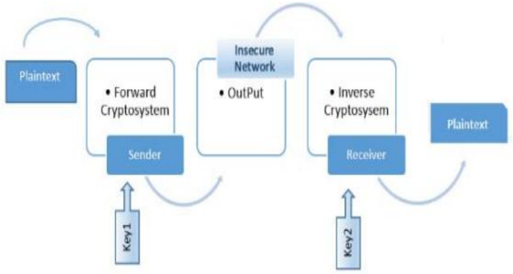

Fig 3 : Cryptography Based Authentication

Advantages

- Conventional cryptography shows fulfilling results for authentication of an image with high tamper detection.

Disadvantages:

- Localization performances are not excellent.
- Hash functions are terribly sensitive.
- Knowledge of private key is must.
- Totally difficult to differentiate between malicious and innocent modification

- Delay in transmission

C. Robust Image Hashing Authentication

The image hashing algorithm is currently wide applied for image authentication. It does not\ modify the content of the initial image. It differs from the standard watermarking methodology that has the contradiction of lustiness and invisibility. Image hashing algorithm relies on image content and may support varied applications like image authentication and retrieval. This methodology is additionally referred to as perceptual hashing, robust hashing etc., and it has received much attention of researchers over the recent years. A typical image hash algorithm consists of two main stages: feature extraction and hash generation. Feature extraction is the crucial step within the algorithm, and it mainly supports spatial domain and transform domain. In hash construction the global and salient local vectors are concatenated to make an intermediate hash. This intermediate hash generates a secret key to supply the ultimate hash sequence [7].

Advantages:

Hashes produced are robust against common image process operations as well as adjusting the brightness, scaling, small angle rotation and noise contamination [7].

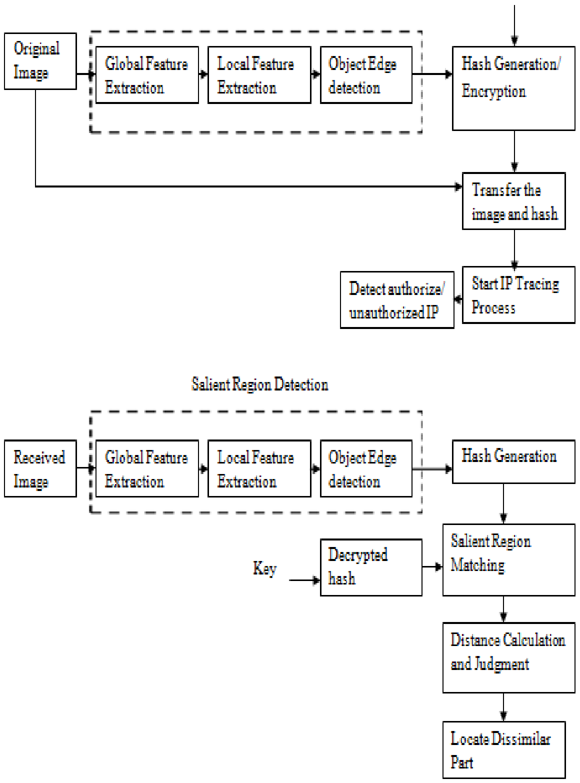

Fig 4: Robust Image Hashing Authentication

IV. CONCLUSION

In this paper various image authentication techniques are discussed. When compared to these three techniques robust image hashing authentication is more effective [4]. We propose to include detailed on study about robust image hashing authentication as a future work.

REFERENCES

[1] https://en.wikipedia.org/wiki/Digital_imaging

[2] IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 1, JANUARY 2013 55 Robust Hashing for Image Authentication Using Zernike Moments and Local Features Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Member, IEEE

[3] http://www.imageforensicexpert.com/digital-image-authentication/

[4] International Journal of Engineering Trends and Technology (IJETT) – Volume 7 Number 4- Jan 2014 ISSN: 2231-5381 http://www.ijettjournal.org Page 184 A Survey on Image Authentication Techniques S.Jothimani1 , P.Betty2 1- PG Scholar, Department of CSE, Kumaraguru College of Technology 2-Assistant Professor, Department of CSE, Kumaraguru College of Technology Coimbatore, Tamil Nadu, India.

[5] http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp199-204.pdf

[6] International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Website: www.ijircce.com Vol. 5, Issue 3, March 2017

[7] A Robust Image Hashing Algorithm Resistant Against Geometrical Attacks YuLing LIU, Yong XIAO College of Information Science and Engineering, Hunan University, Changsha, 410082, China