International Journal of Law
ISSN: 2455-2194
Impact Factor: RJIF 5.12
www.lawjournals.org
Volume 3; Issue 5; September 2017; Page No. 13-18

A techno legal analysis of admissibility of digital photographs as evidence & challenges

[1] Aratrika Chakraborty, [2] Anuradha Parihar
[1] Assistant Professor, Amity Law School, Amity University Kolkata, West Bengal, India
[2] LLM (Cyber Law and Cyber Security), National Law University Jodhpur, Rajasthan, India

Abstract
With the advent of technology, Digital photographs have been able to replace the analog photographs. The concept of photographs was they were captured and required representation on a film or paper. But now the traditional photographs have been replaced with new digital photography where the whole concept of concept of capturing or storing of images is different from the traditional one.
Keeping in view the technology employed in capturing and storing of these digital photographs with the traditional analog images, the rules of admissibility in a court if law differ. Thus, it has to be studied how digital photographs can be made admissible in the court as evidence and the rules corresponding to the same. Time and again photographs have been taken as evidence in the justice delivery system but the question which needs to be addressed is how photographs are made admissible as evidence in the court. In order to answer these questions the provisions of Indian Evidence Act, 1872 in consonance with the Information Technology Act 2000 needs to be studied.
This paper attempts to analyze the principles and some important cases with regard to the authenticity of digital photographs as evidence.

Keywords: digital photograph, admissibility, storing of images

1. Introduction
Pictures are more demonstrative than other documents and can have a greater impact they have been used as a piece of evidence in the courts. The concepts of photographs have also changed with time from traditional analog photographs to the modern day digital photographs. The concept of photographs was they were captured and required representation on a film or paper. But now the traditional photographs have been replaced with new digital photography where the whole concept of concept of capturing or storing of images is different from the traditional one.

1.1 Digital Photographs- Technology and Storage
A computer to if understood technically can be said to be an electronic device which holds a collection or circuits or switches. The computer understands only two things viz. when the circuit is on and when the circuit is off. Thus, computer does not understand the normal user understandable language instead it only understands the language of zeroes and ones which is popularly known as the Binary language. The computer stores information in the form of numbers viz. zero and one which in the binary form are called bits. Any information can be stored or processed only of it is digitized. A computer can store data in two ways: firstly in the primary memory which is the RAM (Random Access Memory); secondly on the magnetic, optical media.
Now moving on to the concept of digital photographs they can be said to exist in the digital form. This would mean that these photographs do not require any film or paper for their generation or storage. The traditional photographs required some kind of analogous representation which is absent in the digital photographs. These photographs are stored in the bits of information known as binary form. Digital photographs are captured in the digital cameras by mapping the scene or image in a grid where different cells are provided with different specifications like intensity of the color etc. An image can be digitized by either scanning an analog image into the computer or a picture can be taken by a digital camera itself. A digital camera looks like a conventional camera itself but the technology employed is different in both. A digital camera contains a sensing apparatus within which calculates numeric value assigned to each pixel.
A digital photograph is substantially different from the conventional photographs as one of the benefit digital photographs is that they can reproduced without any substantial loss in the quality of the photograph which is not the case with the analog image. Since, the image is stored numerically thus the reproduction of any such image would keep the quality of the image intact in both the copy and the original. Also, even while making slight alterations in the image the copies made previously will maintain their authenticity. Also even after this the photographs will remain in the form of numbers meaning in the binary form.
Since the there exists an ease to manipulate digital photographs the court has taken approach where witnesses are sought to provide their opinion over the authenticity of the photographs. The witnesses testify with respect to the fact that the photographs has not been tampered with, in this regard a lot of things come into picture which need to be analyzed like the metadata with respect to the picture etc. A digital

photograph requires a chain of custody form which either proves that the image is original and unaltered or the details of the people who have held the image and the list of alterations made time and again. There is another issue which is addressed by the judiciary in admitting digital photographs as evidence is what should be considered to be "original" copy of the image. Thus at times it has meant to mean the original image if the image in the camera itself is placed before the without any alterations but even a slight manipulation disqualify it to be original.

1.2 Admissibility of photographs as evidence

As it has been already mentioned photographs are considered to be more explanatory in nature or a better of depicting something. Therefore, time and again photographs have been taken as evidence in the justice delivery system but the question which needs to be addressed at this juncture is how photographs are made admissible as evidence in the court. In order to answer these questions the provisions of Indian Evidence Act, 1872 need to be studied.

Section 62, section 63 and 64 deal with the prove of contents of a document and they can be done either by primary or secondary evidence.

Section 62 of Indian Evidence Act, 1872 states that primary evidence means the document itself is placed before the court.

"Primary evidence means the documents itself produced for the inspection of the Court.

Explanation 1—Where a document is executed in several parts, each part is primary evidence of the document:

Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, each counterpart is primary evidence as against the parties executing it.

Explanation 2- Where a number of documents are all made by one uniform process, as in the case of printing, lithography, or photography, each is primary evidence of the contents of the rest; but, where they are all copies of a common original, they are not primary evidence of the contents of the original."

So it can be said that if a photograph if taken and placed directly before the court then it is meant to be primary evidence. But there can be instances where photographs can be said to be secondary evidences also like if the copies are created from the negative of a photograph.

Section 63 deals with secondary evidence:

"Secondary evidence means and includes—

1. *Certified copies given under the provisions hereinafter contained;*
2. *Copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies.*
3. *Copies made from or compared with the original;*
4. *Counterparts of documents as against the parties who did not execute them;*
5. *Oral accounts of the contents of a documents given by some person who has himself seen it."*

Thus photographs of the evidence in original are considered to be secondary evidence. Also photographs can be admitted wither as substantive or demonstrative evidence. Photographs are considered as documents under the evidence act [1]. Substantive evidence is when an evidence proves a fact in issue while demonstrative evidence is when helps to understand the difficult concepts in a case. Thus, if photographs are been taken as substantive evidence then in that case the witness need to testify that the photograph portrays the scene fairly and accurately. Thus, oral evidence in case of photographs is admissible if they are secondary in nature.

2. Determining the authenticity of Digital Photographs

In today's technology driven world the concept of digital photography has come into practice thus nowadays digital photographs have replaced the traditional analogue photographs. Since the entry of these new digital technology relating to photography a lot more aspects and issues have arisen which need to be taken into account and at no instance be ignored. The digital photographs along with its high quality has brought with it the high chances of manipulation in photographs and this has forms the part of concern of the court. These digital photographs since remain in the form of numbers they can be easily altered by way of adding, removing or replacing some of the information. It has been seen and is a common practice where camera man himself makes changes in the photographs and removes features not required. Thus it can be seen that there can be accidental and intentional manipulation of images. Accidental covers those instances like where the storage media of the image is mishandled and as a result of which the image is altered while intentional manipulation of images is when certain elements are removed or added in an image willing like when alterations made by the photographer or the editor in the color contrast of the picture for purely innocent purposes.

Thus keeping in view the above scenario court has issues in admitting digital photographs as evidence and thus it requires testimony of the witnesses to prove the contents but it does not resolve the issues as the testimony itself can be doubted. So, these photographs require a thorough expert analysis. These photographs while being admitted has to go through all the necessary requirements for the admissibility electronic evidence.

With the introduction of digital cameras, there needs to be a stronger requirement of establishment of authenticity to make digital photographs admissible as evidence. Digital photographs pose new issues to the traditional rules of evidence. Though it may appear to be the same as traditional photographs but they are a totally different class of evidence. The digital photographs can be copied any number of times and there is no way to actually distinguish the original from the duplicate one. There may be advertent or inadvertent alterations and it is very difficult to establish the authenticity and that there has been no tampering with the original photograph.

The standard of authentication depends on what purpose the digital photograph is being admitted as evidence. It can be used as substantive evidence or demonstrative evidence. Substantive evidences are used prove directly some facts and demonstrative evidence are used to make something clear or understandable by visually depicting something like X-rays or maps and charts.

2.1 Authentication for substantive Evidence

When authentication for presenting it as a substantive evidence is done the requirements are much more stringent. It has to be proved that it is in the same condition as the original and there has been no tampering. The court relies on the testimony of witnesses that there has been no tampering with the photographs. For the purpose of authentication of a photograph a witness needs to testify that this is an accurate representation of the original. But this testimony may be problematic because either the witness may be examined after many years the photograph was taken, or there may be also chances that the witness may not even know or realize that the photograph has been changed.

- **Chain of Custody:** The chain of custody form may be required to establish he authenticity of the digital photographs. Through a chain of custody form it can be seen the entire log of who handled those digital photographs and for what purpose.
- **Best evidence rule:** The federal rules of Evidence in US require any photograph which is used as a substantive evidence to be in original. This is known as the best evidence rule. So for digital photographs this means that only if the photos are directly taken from the disk drive of the camera itself. However this is not practically possible in most cases, Most of the times it is taken in CDs, or printouts are taken and exact copies can be made of digital photographs without any loss in quality or modification. So the notion of original under the federal rules seems obsolete as far as digital photographs are concerned.
- **Metadata for authentication:** For a typical document, it includes, inter alia, the name of a file, its location on the computer‘s hard drive, the file extension, dates of creation and modification, and names of users who have permission to open or alter a file [2]. The metadata of an image that a digital camera records can include the dimensions of the image, the file size and location, the make and model of the camera used to take the photograph, the focal length and ratio, exposure time, and the dates the photo was taken, last modified, and last opened. Some cameras even have internal GPS chips that record the precise location the picture was taken.

The metadata can serve as important for authentication purposes. The date and time stamping in the camera can establish the proof of fact in issue. However the metadata is not entirely dependable for it can be easily altered or it may not have been saved as accurate in the first place. There can be instances where the date and time of the camera are already set incorrectly in the first place another case is when an image is transferred from the camera to the computer then it reflects the date and time when the image was created in the computer not the original date of creation in the camera. Merely opening or resaving the image file also changes dates in the metadata of the image.

Recent digital cameras have built-in GPS receivers which it possible for the camera to record where exactly a photo was taken. This positioning information (latitude, longitude) can be stored in the Exif metadata header of JPEG files. Tools such as jhead can display the GPS information in the Exif headers. External GPS device can also be connected to the digital camera [3].

- **Hash Value-** By using certain algorithms like MD5 and SHA hash value which is a fixed bit length outcome of the original file can be checked with the copy later made. If the original digital photograph’s hash value is calculated and whenever a copy is made using computer then both their hash values can be compared. Even the slightest change would alter the hash value so this can be used to establish the authenticity of the digital photographs.

2.2 Authentication for demonstrative evidence

When using the digital photographs as demonstrative evidence then the rules are even more relaxed. Demonstrative evidence implicates neither the best-evidence rule, nor chain-of-custody requirements. The danger of fraudulent photographs being admitted as reliable, authentic evidence resents a looming and perplexing dilemma for the legal system [4].

3. Admissibility of digital photographs

3.1 Digital Photographs as Primary Evidence

If the device itself which is storing the electronic evidence is brought before the court then it will be primary evidence and so it will be admitted under S. 62 and not S. 65B.

Under S. 62 of the evidence act the Primary evidence means the document itself produced for the inspection of the Court. As per S. 65 gives the conditions for admitting secondary evidence.S. 65 A and S. 65 B was inserted after this, so this clearly indicates that the electronic evidence is admitted as secondary evidence, not primary evidence.

The media itself in which the recording is made is itself brought before the court then it is primary evidence under S. 62.

If there is a digital photograph stored in a digital camera it is a document within the meaning of S. 3 of the evidence act.

S. 3 of the evidence act says that [all document including electronic records produced for the inspection of the Court, such statements are called documentary evidence;

S per S 2 (t) of the IT Act electronic record is defined as

“(t) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;”

Electronic form is defined in S. 2 (r) of IT Act, 2000:

“Electronic Form with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;”

Digital photographs stored inside the digital camera itself is an electronic record under S. 2(t) of the IT Act, It is images stored in an electronic form, so this is a “document” under S. 3 of the Evidence Act and can be produced as a primary evidence under S. 62 of the Evidence Act.

3.2 Digital photographs as secondary evidence and S. 65B of Information Technology Act, 2000

If the digital photograph is printed, then it becomes creation of an electronic record produced from the digital camera itself pr produced with the help of a computer, where a printout is

taken or it is stored in some media as Cds, DVDs or pendrives. This becomes a secondary digital evidence and then S. 65 B needs to be complied with. Then the functionality of such computer needs to be established and the person who has transferred these photographs and produced them needs to certify.

Functionality test under S. 65 B(2)

S 65 B(2) gives the technical conditions for admissibility

"*(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:-*

a. the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;

b. during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;

c. throughout the materiel part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

d. the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities."

Non-technical qualifications under S. 65B(4)

S. 65 B(4) gives the non-technical qualifying conditions for admissibility of the Secondary digital evidence.

"*(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,-*

a. identifying the electronic record containing the statement and describing the manner in which it was produced;

b. giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;

c. *dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purpose of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it*."

Since in most of the cases the digital camera itself is not produced before the court, either a printout is taken or it is stored in some media like some CDs/ DVDs are prepared. So a person who was responsible in handling of the digital camera and who took the photograph and transferred it to the media needs to certify that how the printout or storage was done and the functionality requirements under S. 65 B (2) was complied with.

In the case of *FIR No. 460/14 : State V/s Mahender : PS Sultan Puri* [5] where an alibi was sought o be established by the defence witness in a rape case, the Delhi district court observed the requirements for the admissibility of digital photographs taken by a digital camera.

The defence witness Ms Versha who claimed to be the girlfriend of the accused stated that the accused was with her at India Gate during the time of the alleged offence by the accused. She testified that from 2 PM to 6 PM the accused was with her and the photographs were taken at 6 PM. For this purpose she placed two digital photographs before the Court which was taken from a digital camera by a private photographer.

The GPS data and the metadata could be used as a proof for the alibi by the defence but the court in this case held that these digital photographs were not admissible. The private photographer was not traced and no certificate under S. 65 B was produced before the court.

The Court relying on *Anwar v Basheer* [6] held that the photographs were not admissible because the witness could not be produced and the digital photographs being Secondary evidence under S. 65 B had to be complied with a certificate. Only if the original evidence as such is placed then there are no requirements under S. 65B.

3.3 Section 45A of the Evidence Act and expert opinion

In India, in S.45A of the Evidence Act, Expert's opinion is sought when genuineness of an electronic record is questioned.

"*Opinion of Examiner of Electronic Evidence. —When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 (21 of 2000) is a relevant fact. Explanation. —For the purposes of this section, an Examiner of Electronic Evidence shall be an expert;"*

As per S. 22A of the evidence Act oral evidence as to contents of an electronic records is admissible only if its genuinity is in question.

The digital photographs can be admitted as primary evidence itself if the digital camera is brought before the court. If its genuity is in question after it being admitted as primary evidence under S. 62 of the Evidence act then expert opinion under S. 45 A of the evidence act can be admissible.

But if a digital photograph is admitted as a secondary evidence then as per the case of *Anvar P.V. v P.K. Basheer & Ors* [7], If a secondary electronic record fulfils the conditions of S. 65B, then expert opinion under S.45A can be sought. As per Para 17 of the judgment

"*17. The Evidence Act does not contemplate or permit the proof of an electronic record by oral evidence if requirements 14 Page 15 under Section 65B of the Evidence Act are not complied with, as the law now stands in India*."

So when a printout of the digital photograph is brought or the media in which it is recorded is sought to be admitted as secondary evidence then expert opinion can be sought only when a certificate under S. 65 B is given.

4. Federal Rules Of Evidence In USA For Authentication

In order to make any documentary evidence admissible the Authentication has to be established. In US the Federal Rules of Evidence, Rule 901 provides for the authentication of an item of evidence sufficient requirements have to be met to support the claim that it is genuine or authentic.

The relevant parts of Rule 901 is

" *Rule 901. Authenticating or Identifying Evidence*

a. *In General. To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.*
b. *Examples. The following are examples only — not a complete list — of evidence that satisfies the requirement:*

(1) Testimony of a Witness with Knowledge. Testimony that an item is what it is claimed to be.

(3) Comparison by an Expert Witness or the Trier of Fact. A comparison with an authenticated specimen by an expert witness or the trier of fact.

(4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances.

(5) Opinion About a Voice. An opinion identifying a person's voice — whether heard firsthand or through mechanical or electronic transmission or recording — based on hearing the voice at any time under circumstances that connect it with the alleged speaker.

(9) Evidence About a Process or System. Evidence describing a process or system and showing that it produces an accurate result."

So when a digital photograph is admitted then opinion of a witness, or an expert is important to make it admissible. Also as per Rule 901(b)(9) a process or system which produces a particular result whether that process is accurate also can be proved by relevant evidence.So when a digital photograph is printed or produced using a computer, the process has to be established as authentic.

4.1 Expert Opinion for Authentication

Rule 702 of the Federal rules talk about the Expert opinion.

"*Testimony by Expert Witnesses*

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

a. *the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;*
b. *the testimony is based on sufficient facts or data;*
c. *the testimony is the product of reliable principles and methods; and*
d. *the expert has reliably applied the principles and methods to the facts of the case."*

4.2 State Of Connecticut V. Alfred Swinton [8].

This case has given new dimensions to the admissibility and authentication of the digital evidence. Though this judgment is binding on the state of Connecticut but can be immense to other states while dealing with digital evidence. In the present case the defendant Alfred Swinton was convicted for the murder of a 28 year old woman. The dead body of the girl was discovered in a partially dressed state, some bite marks were also found on her breasts. Thus, digital photographs were produced as evidence of the marks on the body of the defendant in order to prove that those bite marks was of the defendant.

The photographs of the bite marks were cleared using an image-enhancing software called Lucis. Then these images were compared with the bite-pattern of the defendant by super-imposing over the photographs of the bite-marks using Adobe Photoshop. Swinton appealed on the basis that the images were improperly admitted because of the use of Lucis and Adobe Photoshop.

In order to analyze Swinton's claims the court followed a six-factor test which is illustrated below [9]:

1. *The computer equipment is accepted in the field as standard and competent and was in good working order,*
2. *Qualified computer operators were employed,*
3. *Proper procedures were followed in connection with the input and output of information,*
4. *A reliable software program was utilized,*
5. *The equipment was programmed and operated correctly, and*
6. *The exhibit is properly identified as the output in question*

The court came up with the principles for authentication standards for the computer-generated evidence and applied then in two parts of evidence: the photographs enhanced through Lucis and Adobe Photoshop. The Court defined Rule of Law and applied the rule on the two pieces of evidence

a) Lucis-Enhanced Photographs: The testimony of a forensic scientist was used in order to admit these photographs. The Court applied the six-factor test to the testimony of the forensic scientist and concluded that the digitally enhanced photographs were sufficiently authenticated. Court observed that:

- The computer equipment used was the standard equipment;
- Through the experience and training of the witness and presence of Karazual proves that the enhancement was produced by a qualified computer operator;
- Proper input and output procedures were followed;
- Lucis was a reliable software program

b) Adobe Photoshop Overlays: this part analyzed the testimony of Karazulas for the evidence created by Adobe Photoshop. His testimony was based on four levels of bitemark comparison:

- molds that demonstrated unique characteristics;
- regular photographs that allowed the deduction of the victim and assailant's positioning;
- a comparison of the molds and the photographs; and
- Adobe Photoshop-enhanced overlays.

The Court held that the testimony here was insufficient to prove that the authentication was made in a proper manner because he failed to prove five out of the six factor test.

5. Conclusion

Since the technology of digital photographs is comparatively new, rules of authentication and admissibility are also

evolving and judicial decisions are helping to set the standards regarding the admissibility of Digital photographs as evidence. Digital photographs are electronic records in electronic form so there needs to be proper amendments in existing laws to accommodate the insertion of digital photographs in the ambit of evidences pertaining to electronic form. In US as the case of *State v. Swinton* [10] has been a landmark decision in determining the authentication and admissibility principles of digital photographs, In India as of now *Anvar v. Basheer* [11] stands as the law and S. 65 B requirements have to be met for admitting the digital photographs in court.

References

1. See, Section 3 of Indian Evidence Act, 1872
2. Case Blurb: Lorraine; Authenticating ESI Under FRE 901(b)(4) by Examining Metadata, 2007. available at,http://postprocess.wordpress.com/2007/09/18/case-blurb-lorraine-authenticating-esi-under-fre-901b4-by-examining-metadata/
3. Emerick D. Jobo announces GPS digital camera add-on, 2008. available at, http://emerick.blogspot.com/ 2008_02_01_archive.html
4. Zachariah B Parry. Digital Manipulation and Photographic Evidence: Defrauding Courts One thousand words at a time, Journal of Law, Technology & Policy, 2009.
5. DOD: 22.07.2015, (Sessions Case No. 111/14), Unique ID case No.02404R0166232014
6. Civil Appeal No. 4226/2012 (DOD: 18.09.2014)
7. Ibid
8. Case: 847 A.2d 921(Conn. 2004)
9. Supra note 3
10. Supra Note 8
11. Supra Note 6