

Review of Digital Image Forgery Detection Tools

Ashok Nayak.B & Dr.E.Nagabhooshanam

Department Of ECE PHD In Digital Image Processing, Osmania University, Telangana, Hyderabad, India.

ashoka405@gmail.com

Professor, ECE Dept, CMR Engineering College, Telangana, Hyderabad, India.

enb1234@gmail.com

Abstract: Digital image forgery is one of the outstanding field in which can easy to control image from multiple points of view using several capable image processing and editing software's. A mid the past decade effective computers, high-resolution digital cameras and photograph editing software packages have turned out to be accessible to countless. As a result, it has turned out to be genuinely straightforward to make digital image forgeries that are difficult to distinguish from real images and surprising difficulties on control image. Effects of forgeries, in the mass media or courts of law can importantly affect our society. As a result. It becomes a serious social problem. The researchers continuously exploring new approaches to detect image tampering areas and Under this assumption, This work analyze to propose techniques that quantify what's more, identify factual annoyances found in two distinct types of forgery images, picture with copied The availability of serious digital picture processing programs, for example, Photoshop, makes it modestly simple to make digital phonies from one or different images. An instance of a digital picture forgery is appeared in figure-1. As the newspaper set pattern shows, three unique photographs were used in making the composite image as with image of the White House, Bill Clinton and Saddam Hussein. The White House was resealed and obscured to make an illusion of an out-of-focus foundation. By then, Bill Clinton and Saddam were cut off from two particular images and glued on the White House picture. Care was taken to get the speaker remains with mouthpieces while safeguarding the correct shadows and lighting. Figure-1 is, truth be told, a case of an exceptionally realistic looking forgery.

areas (e.g., Copy-Move image Forgery) and Re-sampled images(e.g., scaled or rotated image Forgery). For every method build up the hypothetical establishment, show its effectiveness on dependable forgeries, and break down its sensitivity and robustness to simple counter-attacks. These techniques plays a crucial part in application to Mass Media and Court of Law, Military and Intelligence agencies, Criminals, Law requirement and counter intelligence agencies. In this paper to discuss review and new trends, state of art on the detection of image forgery techniques.

Keywords: Digital image forgery; tampering areas; Duplicated regions; Re-sampled images; Block matching algorithms.

1. INTRODUCTION:



Fig-1: Example of a digital forgery.

Tampering with images is something neither new, nor recent. Some of the most well known examples of falsification image are shown below fig-2.



Fig-2: Forged "Hats" image

These are comparative; fabrications were made utilizing picture controls, for example, artificially glamorizing, re-touching, dodging and expanding, and difference and shading change.

Despite the way that the requirement for identification of digital forgeries has been perceived by the research group, here have not very many publications are as of now accessible. The basic learning required around one approach is digital watermarks have been proposed as a means for delicate validation, content confirmation, discovery of altering, limitation of changes and recuperation of unique substance. While digital watermarks can give helpful information about the picture trustworthiness and its processing history, the watermark must be available in the picture before the adjusting happens. This constrains their application to controlled conditions that consolidate military frameworks or surveillance cameras. Unless all digital acquisition devices are furnished with a watermarking chip, it will be far-fetched that a forgery-in-the-wild will be discernible using a watermark.

STATE OF ART:

A digitally changed photo, regularly leaving no visual clues of having been messed with can be indistinguishable from a genuine photo. Amid the past decade, intense computers, high-resolution digital cameras and sophisticated photograph editing software packages have turned out to be moderate and open to a far reaching number of people. As a result, it has

turned out to be genuinely straightforward to make digital forgeries that are difficult to distinguish from legitimate photographs. These falsifications, if utilized as a part of media or courts of law, can imperatively influence our general public. This photo, however was not valid it was made by digitally splicing together two distinct photographs. We depict a few measurable systems for recognizing hints of digital modifying without any digital watermark or mark. Specifically, we evaluate statistical correlations that result from specific forms of digital altering and devise identification schemes to uncover these correlations.

2. LITERATURE SURVEY:

Detecting digital tampering in the absence of watermarks or signatures is a relatively new research topic and only few results have been published so far. Farid proposed a technique for authenticating digital audio signals. This system works under the suspicion that characteristic signs have low higher-order correlations in the frequency domain [1]. He then showed that higher-order correlations are introduced in the frequency domain when a natural audio signal undergoes a nonlinear transformation, as would likely happen in the process of creating a digital forgery. Tools from polyspectral analysis, i.e., the bispectrum were applied to quantify and detect these correlations. This approach was extended by Ng and Chang [2] to detect splicing in composite images. Farid and Popescu have also applied this technique to blindly detect the presence of multiple nonlinearities in digital images [3], which represents a possible sign of tampering. Lyu and Farid have proposed a method to distinguish between photographic and computer generated, photo-realistic images. Their method works by representing an image with a multiscale, multi-resolution, wavelet-like transform, then extracting a feature vector of first and higher order statistics from the transform coefficients. Statistical learning tools (e.g., linear discriminate analysis and non-linear support vector machines) are employed on these feature vectors to discriminate between photographic and photo-realistic images.

3. METHODOLOGY:

3.1 Proposed System

A mid the past couple of years moderate, high-resolution digital cameras have been quickly supplanting their film-based, simple counterparts. What's more, the approach of ease, high execution computers, and sophisticated photograph editing and PC graphics software enable a normal user to do complex image manipulations and make trustworthy digital forgeries without lifting a finger. Despite the fact that there are, perhaps, an uncountable number of ways to control and mess with digital images, we present here some of the most well-known types of digital image tampering.

In this paper to discuss review and new trends on the detection of image forgery techniques of this work analyze to propose techniques that quantify and detect statistical perturbations found in two different forms of forgery images, image with duplicated regions(e.g., Copy-Move image Forgery) and Re-sampled images(e.g., scaled or rotated image Forgery). We describe a set of statistical techniques for detecting traces of tampering in digital images. These systems work in the entire nonattendance of any digital watermark or mark. The common theme and unifying framework, of these techniques is the assumption that digital forgeries, often visually imperceptible, alter some underlying statistical properties of natural images. Within this framework, our approach consists in first identifying the statistical changes associated with particular kinds of tampering, then designing techniques for estimating these changes. Following this approach, we have developed two techniques for that quantify and detect different types of tampering:

A) Duplicated Image Regions: A common manipulation in removing an unwanted person or object from an image, is to copy and paste portions of the same image over the desired region. On the off chance that the grafting is vague, little concern is regularly given to the way that indistinguishable areas are available in the picture. Copied areas are then distinguished by lexicographical arranging all DCT square coefficients. In a Copy-Move forgery, a piece of the picture itself is reordered into another piece of a similar picture. This is usually performed with the intention to make an object “disappear” from the image by covering it with a segment copied from another part of the image. Completed ranges, for example, grass, foliage, shake, or surface with sporadic examples, are ideal for this reason in light of the fact that the copied regions will most likely blend with the establishment and the human eye can't without much of a stretch perceive any suspicious antiquities. Because the replicated parts originate from the same image, its noise segment, shading palette, dynamic range, and most other vital properties will be perfect with the rest of the image and thus won't be discernible using methods that search for incompatibilities in statistical measures in various parts of the image. To influence the forgery much harder to identify, one to can use the feathered product or the modify apparatus to additionally mask any traces of the replicated and-moved segments.



Fig-3: Original Jeep image and Lina image



Fig-4: Forged Jeep image and Forged Lina image

B) Discussion and Results:

Cases of Copy-Move forgery are given in Fig-3. In Fig-3 Jeep picture, you can see a more subtle forgery in which a truck was secured with a segment of the foliage left of the truck (contrast the fashioned picture and its unique). In Figure 3 Lina image, you can see more obviously that

some part of the image is copied and pasted and you can detect duplicated regions very easy in this image. Discovery of Copy-Move Forgery by block Matching procedure, create comes about with Exact Matching. Consider a gray-scale image with N pixels (we discuss below how this algorithm extends to color images). An

image is tiled with overlapping blocks of b pixels ($\sqrt{b} \times \sqrt{b}$ pixels in size), each of which is assumed to be considerably smaller than the size of the duplicated regions to be detected. Arrange these blocks into a two-dimensional array A of size $N_b \times b$, where $N_b = (\sqrt{N} - \sqrt{b} + 1)^2$. Each row corresponding to one position of the sliding

block. Two identical rows in the matrix A correspond to two identical $\sqrt{b} \times \sqrt{b}$ blocks. To identify the identical rows, the rows of the matrix A are lexicographically sorted (as $\sqrt{b} \times \sqrt{b}$ integer tuple). This can be done in $O(N \log N)$ steps.



Fig-5: Shown are the results of Exact Matching Algorithm after applying on Jeep image and Lena image.

The matching rows are easily searched by going through all N rows of the ordered matrix A and looking for two consecutive rows that are identical. The matching blocks found in the BMP image of Jeep and Lena image for both $b=64$ are shown in Figure 5. Note that if the forged image had been saved as JPEG, vast

majority of identical blocks would have disappeared because the match would become only approximate and not exact. This also why the exact match analysis of images from There is did not show any exactly matching blocks. In the next section, the algorithm for the robust match is given and its performance evaluated

3.2 Proposed System

A) Re-sampled Images: Imagine a forgery created by splicing together images of two people and overlaying them on a chosen background. Keeping in mind the end goal to make a persuading match it is frequently important to re-measure, turn, or extend the first images (or segments of them), which requires re-examining the images onto an alternate cross section. Re-inspecting presents particular relationships between's neighboring picture pixels that are measured and distinguished utilizing the desire augmentation (EM) calculation. Consider the situation in which a digital forgery is made by grafting together at

least two images. In order to create a convincing match, it is often necessary to re-size, rotate, or stretch the images, or portions of them. This procedure typically requires re-sampling an image onto a new sampling lattice using an interpolation technique (e.g., bi-cubic). In spite of the fact that a re-examined picture is frequently vague, it contains particular connections that, when recognized, may speak to proof of altering. We portray the type of these relationships, and propose a calculation for recognizing them in any segment of an image. For motivations behind work we will initially portray how and where re-testing presents connections in 1-D signs, and how to recognize

these relationships. The moderately direct speculation to 2-D images is then displayed. To delineate the general adequacy of this procedure, we indicate comes about on re-inspected characteristic test images and on perceptually trustworthy imitations. Likewise introduced is a broad arrangement of trials that test the affectability of re-examining location for an expansive arrangement of parameters, and additionally the procedure's power to basic counter-assaults and lossy image compression schemes.

Re-sampling signals

Consider a 1-D discretely-sampled signal $x[t]$ with m samples, Fig-6(a). The number of samples in this signal can be increased or decreased by a factor p/q to n samples in three steps:

1. **up-sample:** Create a new signal $x_u[t]$ with pm sample, where $x_u[pt] = x[t]$, $t=1, 2, m$, and $x_u[t]=0$ otherwise, Fig-6(b).

2. **Interpolate:** convolve $x_u[t]$ with a low-pass filter: $x_i[t] = x_u[t] * h[t]$, Fig-6(c).

3. **down-sample:** create a new signal $x_d[t]$ with n samples, where $x_d[t] = x_i[qt]$,

$t=1,2,\dots,n$. Denote the re-sampled signal as $y[t] = x_d[t]$, Fig-6(d).

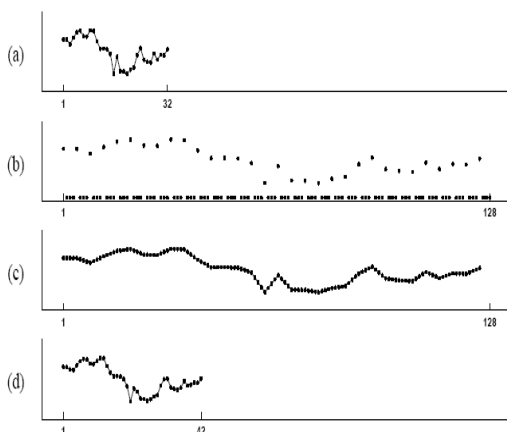


Fig-6: Re-sampling a signal 4/3 factor: shown are [a] the original signal; [b] the up-sampled signal; [c] the interpolated signal; and [d] the final re-sampled signal.

Detecting Re-sampling

Given a signal that has been re-sampled by a known amount and interpolation method, it is possible to find a set of periodic samples that are correlated in the same way to their neighbors. For example, consider again the re-sampling matrix of Equation (1). The specific form of the correlations can be determined by finding the neighborhood size, N , and the set of coefficients, $\vec{\alpha}$, that satisfy:

$$\vec{a}_i = \sum_{k=-N}^N \alpha_k \vec{a}_{i+k}, \text{ where } i^{\text{th}} \text{ row of the re-sampling matrix and } i = 3, 7, 11, \text{ etc.}$$

If, on the other-hand, we know the specific form of the correlations, $\vec{\alpha}$, then it is straightforward to determine which samples satisfy $y_i = \sum_{k=-N}^N \alpha_k y_{i+k}$.

By and by, obviously, neither the examples that are corresponded, nor the particular type of the connections are known. To decide whether a flag has been re-examined, we utilize the desire augmentation algorithm1 (EM) to all the while appraise an arrangement of intermittent examples that are associated to their neighbors, and the particular type of these relationships. We start by accepting that each example has a place with one of two models. The principal displays, M1, compares to those examples that are connected to their neighbors, i.e., are produced by the accompanying model:

$$M1: y_i = \sum_{k=-N}^N \alpha_k y_{i+k} + n(i) \quad (1)$$

Where the model parameters are given by the specific form of the correlations, $\vec{\alpha}(\alpha_0 = 0)$, and $n(i)$ denote independently, and identically distributed (I.I.D) samples drawn from a Gaussian distribution with zero mean and unknown variance σ^2 . The second model, M2, corresponds to those samples that are not correlated to their neighbors, i.e., are generated by an outlier process. The EM algorithm is a two-step iterative algorithm: (1) in the E-step the

probability that each sample belongs to each model is estimated; and (2) in the M-step the specific form of the correlations between samples is estimated. More specifically, in the E-step, the probability of each sample y_i belonging to model $M1$ can be obtained using Bayes' rule:

$$\Pr\{y_i \in M1 | y_i\} = \frac{\Pr\{y_i | y_i \in M1\} \Pr\{y_i \in M1\}}{\sum_{k=1}^2 \Pr\{y_i | y_i \in M_k\} \Pr\{y_i \in M_k\}} \quad (2)$$

Where the priors $\Pr\{y_i \in M1\}$ and $\Pr\{y_i \in M2\}$ are assumed to be equal to 1/2. The probability of observing a sample y_i knowing it was generated by model $M1$ is given by:

$$\Pr\{y_i | y_i \in M1\} = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{\left(y_i - \sum_{k=-N}^N \alpha_k y_{i+k}\right)^2}{2\sigma^2}\right] \quad (3)$$

We assume that the probability of observing samples generated by the outlier model, $\Pr\{y_i \in M2\}$, is uniformly distributed over the range of possible values of y_i . The variance, σ^2 , of the Gaussian distribution in Equation (3) is estimated in the M-step (see Section-B). Note that the E-step requires an estimate of $\vec{\alpha}$, which on the first iteration is chosen randomly. In the M-step, a new estimate of $\vec{\alpha}$ is computed using weighted least-squares, that is, minimizing the following quadratic error function:

$$E(\vec{\alpha}) = \sum_i w(i) \left(y_i - \sum_{k=-N}^N \alpha_k y_{i+k} \right)^2 \quad (4)$$

Where the weights $w(i) = \Pr\{y_i \in M1 | y_i\}$, Equation(2), and $\alpha_0 = 0$. This error function is minimized by computing the gradient with respect to $\vec{\alpha}$, and setting the result equal to zero. Solving for $\vec{\alpha}$ yields:

$$\vec{\alpha} = (Y^T W Y)^{-1} Y^T W \vec{y} \quad (5)$$

Where the matrix is:

$$Y = \begin{bmatrix} y_1 & \cdots & y_n & y_{N+2} & \cdots & y_{2N+1} \\ y_2 & \cdots & y_{N+1} & y_{N+3} & \cdots & y_{2N+2} \\ \vdots & & \vdots & \vdots & & \vdots \\ y_i & \cdots & y_{N+i-1} & y_{N+i+1} & \cdots & y_{2N+i} \\ \vdots & & \vdots & \vdots & & \vdots \end{bmatrix} \quad (6)$$

And W is a diagonal weighting matrix with $w(i)$ along the diagonal. The E-step and the M-step are iteratively executed until a stable estimate of $\vec{\alpha}$ is achieved see Section B for a detailed algorithm. The final $\vec{\alpha}$ has the property that it maximizes the likelihood of the observed samples.

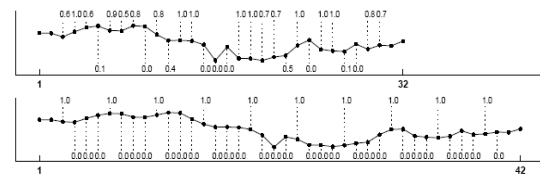


Fig-7: A signal with 32 samples (top) and this signal re-sampled by a factor of 4/3 using cubic interpolation (bottom).

Each sample is annotated with its probability of being correlated to its neighbors. Note that for the up-sampled signal these probabilities are periodic, while for the original signal they are not. Shown in Figure 6 are the results of running EM on the original and re-sampled signals of Figure 5. Shown on top is the original signal where each sample is annotated with its probability of being correlated to its neighbors (the first and last two samples are not annotated due to border effects a neighborhood size of five, $N = 2$, was used in this example). Similarly, shown on the bottom is the re-sampled signal and the corresponding probabilities. In the latter case, the periodic pattern is obvious: only every 4th sample has probability 1, as would be expected from an up-sampling by a factor of 4/3. As expected, no

periodic pattern is present in the original signal. The periodic pattern introduced by re-sampling depends, of course, on the re-sampling rate. As a result, it is possible to not only uncover traces of re-sampling, but to also estimate the amount of re-sampling. There are, however, parameters that produce indistinguishable periodic patterns, which means that the amount of re-sampling can be estimated only within an inherent ambiguity. Since we are primarily concerned with detecting traces of re-sampling, and not necessarily the amount of re-sampling, this limitation is not critical.

B) Discussion and Results:

In the previous sections we showed that for 1-D signals re-sampling introduces periodic correlations, and that these correlations can be detected using the EM algorithm. The extension to 2-D images is relatively straightforward. As with 1-D signals, the up-sampling or down-sampling, of an image is still linear and involves the same three steps: up-sampling, interpolation, and down sampling these steps are simply carried out on a 2-D lattice. Again, as with 1-D signals, the re-sampling of an image introduces periodic correlations. Though we will only show this for up and down-sampling, the same is true for an arbitrary affine transform. Consider, for example, the simple case of up-sampling by a factor of two. Shown in Fig-6 are, from left to right, a portion of an original 2-D sampling lattice, the same lattice up-sampled by a factor of two, and a subset of the pixels of the re-sampled image. Assuming linear interpolation, these pixels are given by:

$$\begin{aligned}
 y_2 &= 0.5y_1 + 0.5y_3 \\
 y_4 &= 0.5y_1 + 0.5y_7 \\
 y_5 &= 0.25y_1 + 0.25y_3 + 0.25y_7 + 0.25y_9,
 \end{aligned}
 \tag{7}$$

And where $y_1 = x_1, y_3 = x_2, y_7 = x_3, y_9 = x_4$. Note that the pixels of the re-sampled image in the odd rows and even columns (e.g., y_2) will all

be the same linear combination of their two horizontal neighbors. Similarly, the pixels of the re-sampled image in the even rows and odd columns (e.g., y_4) will all be the same linear combination of their two vertical neighbors. That is, as with 1-D signals, the correlations due to re-sampling are periodic. A 2-D version of the EM algorithm can then be applied to uncover these correlations in images. For the results presented here, we employed approximately 20 gray-scale images in TIFF format, both 512×512 pixels in size. Using bi-cubic interpolation these images were up-sampled, down-sampled, rotated, or affine transformed by varying amounts. For the original and re-sampled images, the EM algorithm described in Section 'B' was used to estimate probability maps that embody the correlations between pixels and their neighbors. The EM parameters were fixed throughout at $N=2, \sigma_0=0.0075, N_h=3^5$ and $p_0=1/256$ (see Section-B). Shown in Fig-(9-10) are several examples of the periodic patterns that emerged due to re-sampling. In the top row of each figure are (from left to right) the original image, the estimated probability map and the magnitude of the central portion of the Fourier transform of this map (for display purposes, each Fourier transform was independently auto-scaled to fill the full intensity range and high-pass filtered to remove the lowest frequencies). Shown below this row is the same image uniformly re-sampled at different rates? For the re-sampled images, note the periodic nature of their probability maps and the strong, localized peaks in their corresponding Fourier transforms.



Fig-8: Shown from left to right are: a portion of the 2D lattice of an image, the same lattice up-sampled by a factor of 2, and a portion of the lattice of the re-sampled image.

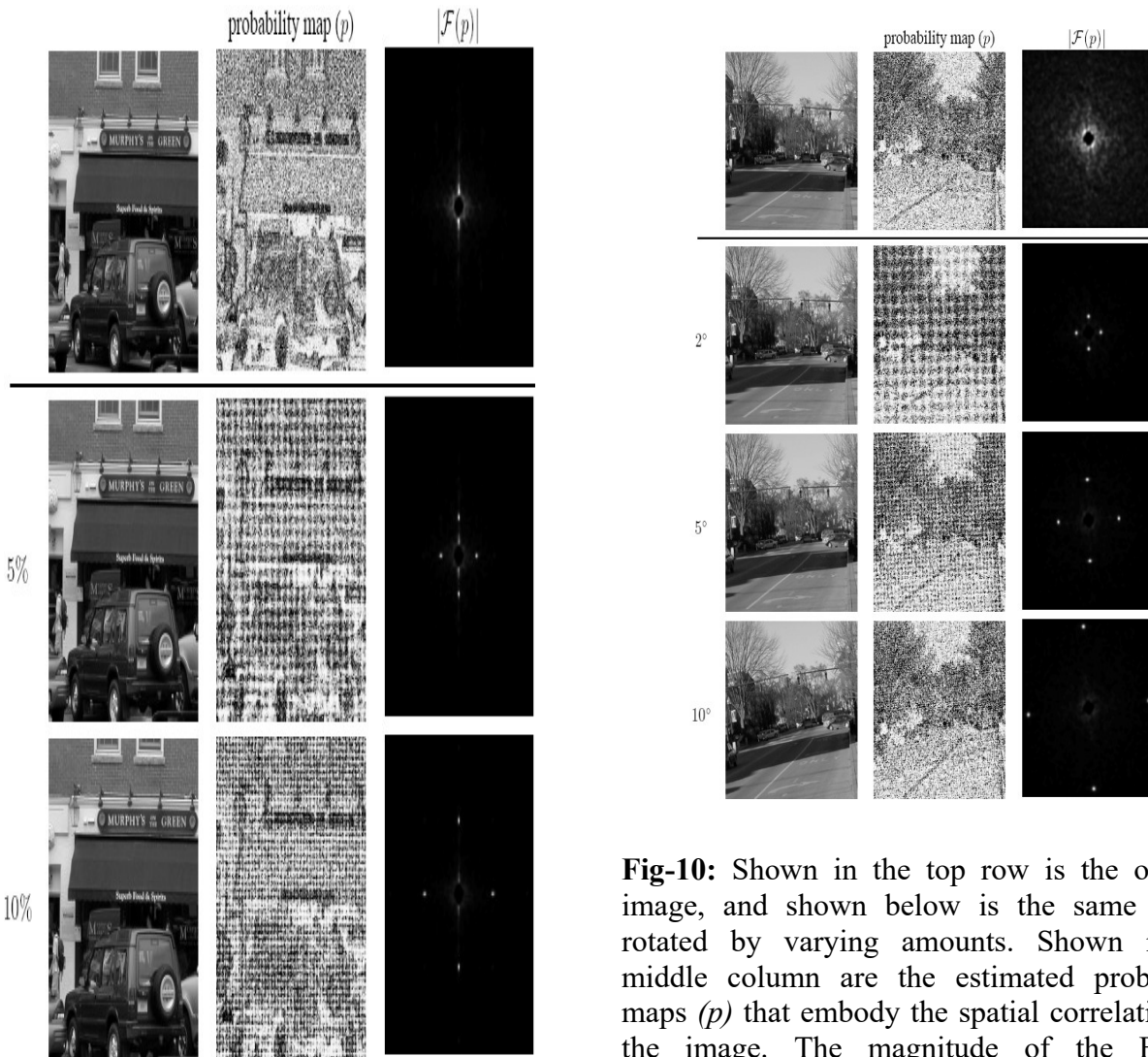


Fig-9: Shown in the top row is the original image, and shown below is the same image up sampled by varying amounts. Shown in the middle column are the estimated probability maps (p) that embody the spatial correlations in the image. The magnitude of the Fourier transform of each map is shown in the right-most column. Note that only the re-sampled images yield periodic maps.

Fig-10: Shown in the top row is the original image, and shown below is the same image rotated by varying amounts. Shown in the middle column are the estimated probability maps (p) that embody the spatial correlations in the image. The magnitude of the Fourier transform of each map is shown in the right-most column. Note that only the re-sampled images yield periodic maps. Shown in below figures are the results from applying consecutive re-samplings. Specifically, the image in the left column is the result of up-sampling by 5%, 10% an original image and then rotating by 2° , 5° and 10° the up-sampled image. The same operations were performed in reverse order on the same original image to yield the image in the right column. Note that while the images are perceptually indistinguishable, the periodic patterns that emerge are quite distinct, with the last re-sampling operation dominating the pattern. Note also that the corresponding Fourier transforms contain several sets of peaks corresponding to both re-sampling operations. As with a single re-sampling, consecutive re-

Samplings can be easily detected. Shown in Figures 9 and is the example of our detection algorithm applied to images where only a portion of the image was re-sampled. Regions in each image were subjected to a range of stretching, rotation; shearing, etc. (these manipulations were done in *Adobe Photoshop®*). Shown in each figure is the original photograph, the forgery (where a portion of the original is replaced or altered), and the estimated probability map. Note that in each case, the re-sampled region is clearly detected while the periodic patterns are not particularly visible in the spatial domain at the reduced scale, the well localized peaks in the Fourier domain clearly reveal their presence (for display purposes, each Fourier transform was independently auto-scaled to fill the full intensity range and high-pass filtered to suppress the lowest frequencies). Note also that in Figures the white sheet of paper on top of the trunk has strong activation in the probability map when seen in the Fourier domain; however, it is clear that this region is not periodic, but rather uniform, and thus not representative of a re-sampled region

4. FUTURE SCOPE OF WORK:

In this paper we are discuss with the review and state of art on work, trends on detection for image forgery techniques to avoid the effects of noise in images, also discuss the different types of the objective identification methods and improve the performance of the resolution of images. The future work of this research work is to identify the static forgery image and to enhance the performance image resolution.

BIBLIOGRAGPY

1. J. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking*. Morgan Kaufmann Publishers, 2002.
2. J. Cox, M. L. Miller, J. M. G. Linnartz, and T. Kalker. *Digital Signal Processing for Multimedia Systems*, chapter A Review of Watermarking Principles and Practices., Marcel Dekker, 1999.
3. CV. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel. Lossless recovery of an original image containin embedded data. U.S. Patent Application,E-D, 1999.
4. JK. Fridrich, M. Goljan, and M. Du. Invertible authentication. In *Proceedings of SPIE, Security and Watermarking of Multimedia Contents*, 2001.
5. C.-Y. Lin and S.-F. Chang. A robust image authentication algorithm surviving JPEG lossy compression. In *SPIE Storage and Retrieval of Image/Video Databases*, 1998.
6. Schneider and S.-F. Chang. A robust content-based digital signature for image authentication. In *IEEE International Conference on Image Processing*, volume 2, pages 227–230, 1996.
7. D. Storck. A new approach to integrity of digital images. In *IFIP Conference on Mobile Communication*, pages 309–316, 1996.
8. BD. M. Macq and J.-J. Quisquater. Cryptology for digital TV broadcasting. *Proceedings of the IEEE*, 83(6):944–957, 1995.
9. MK. U. Celik, G. Sharma, E. Saber, and A. M. Tekalp. Hierarchical watermarking for secure image authentication with localization. *IEEE Transactions on Image Processing*, 11(6):585– 595, Jun 2002.
10. MV. Yeung and F. Mintzer. An invisible watermarking technique for image verification. In *Proceedings of the International Conference on Image Processing*, 1997.
11. JR. Fridrich and M. Goljan. Images with self-correcting capabilities. In *Proceedings of the IEEE International Conference on Image Processing*, 1999.
12. S. Bhattacharjee and M. Kutter. Compression-tolerant image authentication. In *IEEE International Conference on Image Processing*, volume 1, pages 435–439, 1998.
13. DE. Kundur and D. Hatzinakos. Digital watermarking for tell-tale tamper proofing and authentication. *Proceedings of the IEEE*, 87(7):1167–1180, 1999.

14. GG.-J. Yu, C.-S. Lu, H.-Y. M. Liao, and J.-P. Sheu. Mean quantization blind watermarking for image authentication. In *IEEE International Conference on Image Processing*, volume 3, pages 706–709, 2000.
15. PP. W. Wong. A watermark for image integrity and ownership verification. In *Proceedings of IS&T PIC Conference*, pages 374–379, Portland, Oregon, May 1998.
16. J. Fridrich. Security of fragile authentication watermarks with localization. In *Proceedings of SPIE, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents*, volume 4675, pages 691–700, Jan 2002.
17. SK. Katzenbeisser and F. A. P. Petitcolas. *Information Techniques for Steganography and Digital Watermarking*. Artec House, 2000.
18. MV. Wu and B. Liu. Watermarking for image authentication. In *IEEE International Conference on Image Processing*, 1998.
19. GR. L. Friedman. The trustworthy camera: Restoring credibility to the photographic image. *IEEE Transactions on Consumer Electronics*, 1993.
20. P. W. Wong. A public key watermark for image verification and authentication. In *IEEE International Conference on Image Processing*, volume 1, pages 455–459, 1998.