International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-5S, May 2019

An Effective Authentication Scheme for Videos using Invisible Watermark

Jayati Bhadra, M. Vinayaka Murthy, M.K. Banga

Abstract: ***In this paper, a novel reversible keyless invisible authentication method for video piracy protection which uses randomized pixel for embedding real identity information is proposed. Randomization at two different levels is not considered in any of the existing methods. Videos, with this proposed embedding of authentication information, ensure minimum distortions and maximum resistance to the removal of authentication information. Keyless invisible embedding process increases the security and reduces the cost. This proposed approach enhances the randomization of the specific pixels where authentication information will be stored in a frame and the location of such modified pixels is stored in an immediate next frame. Each pair is identified with an embedded random number. Modified Least Significant Bit (LSB) based invisible watermark mechanism is used to embed the bits which are cost effective due to simplicity and which can withstand statistical attacks. During extraction, frame with pixel locations is used. The extracted information will be compared to assure the authenticity of video. The Euclidean distance, PSNR, MSE, SSIM proved that the proposed method can withstand visual attacks. StirMark test proved that the proposed algorithm is highly robust.***

Index Terms: ***Modified Least Significant Bit, Invisible Watermark, Video Authentication***

I. INTRODUCTION

In this era of deep penetration of internet connectivity and smartphones, images and videos have taken the center stage as a media for communication, entertainment, etc. Every instance, a mind-boggling number of images/videos is being transmitted using internet. Naturally, such large volume of image/video exchanges has brought copyright protection the most important aspect resulting in such contents being embedded with copyright information in various forms using different mechanisms. Videos, with such embedded copyright information, require minimum distortions and maximum resistance to the removal of authentication information for effective control of the rampant piracy menace that is prevalent currently. Any video is composed of a sequence of still images and audio tracks. It can be broken up into image frames and audios. Each image frame consists of a set of pixels. Each pixel is having set of intensity information bits. As such, it is easier to hide sensitive privacy information in a video compared to other media. LSB method is the most common, simple but effective method with low computational complexity in Spatial Domain. Identification of pixels where the authentication information has to be embedded and selection of embedding method are the most important criteria for this scheme. After embedding, the resultant frames should have minimized distortion so that utmost protection from visual and statistical attacks shall be observed. The existing lossless embedding processes generally use Pseudo Random Number Generator (PRNG) [9] for selecting the pixels simple but effective method with low computational complexity to embed secret message and LSB[10] of those pixels' intensity values will store the bits of authentication information, though they are vulnerable to statistical attacks. In this paper a modified LSB instead of only LSB and the pixels of Red color channel of the frames are used. Two layers of influence circles instead of energetic pixel [7, 8] concept is used to randomize the pixel selection for embedding which increases the computational complexity. In turn, it increases the security of the embedded information.

II. RELATED WORK

Video watermark algorithms are generally based on relationships between frames and different types of embedding. LSB steganographic method is a very simple but effective method with low computational complexity to embed secret message. Ramalingam et al. [1] used modified LSB algorithm for better efficiency. Bin et al. [2] proposed a data encapsulation method based on motion vectors by using matrix encoding in video. Cao et al [3] proposed a video watermark algorithm based on motion vector as carrier for data hiding method and H.264 video compression process. The principle of "linear block codes" is used here to reduce transformation rates of motion vectors. Kelash et al [4] proposed an algorithm to directly embed data into video frames using color histogram, where pixels of each video frame will be partitioned into two halves, right half will contain hidden bits and left half will contain the counts of right half. Feng B et al. [5] proposed" the syndrome trellis code (STC) with flipping distortion measurement" which compromises capacity but solves the security issue. Tashk A et al. [6] proposed "modified duel watermark scheme" which is in transform domain and gives excellent recovery capacity. The scheme is having computational complexity. Paul et al. [7] uses one bit per pixel for LSB based insertion inside energetic pixel. Paul et al. [8] proposed dynamic optimal multi-bit image steganography using energetic pixels and Ising energy concept and hiding bits of the secret message in the higher bit planes of image pixels which are high-energetic in nature. This scheme can be considered as an embedding process. In this scheme, high embedding capacities are considered over gray scale image. However, all the three planes of color image are not exploited. Also it is implemented on uncompressed images.

Manuscript published on 30 May 2019.
* Correspondence Author (s)
Ms. Jayati Bhadra earned, St. Joseph's College (Autonomous) Bangalore.
Dr M VINAYAKA MURTHY, REVA University, India.
Dr. M.K BANGA, Dayanand Sagar University, India.

III. METHODOLOGY

Rule 1: We define the distance_row of a particular pixel as the difference of the index value of the row of a particular pixel and that of other pixel.

Rule 2: We define the distance_column of a particular pixel as the difference of the index value of the row of a particular pixel and that of other surrounding pixels in influence circle.

Rule 3: We define the influence_distance as the maximum distance_row or distance_column of between a specific pixel and its surrounding pixels.

Let us consider that value of a specific pixel be $P_{i,j}$ and an arbitrary pixel from its be $Q_{k,l}$. Let us assume a, b are the distance_row and distance_column respectively. Then

Either k-i ≤ 0 or k-i = a where 0 ≤ a ≤ 2 and 0≤ i, k ≤ 2

Either l-j ≤ 0 or l-j = b where 0 ≤ b ≤ 2 and 0≤ j, l ≤ 2……(1)

Since influence_distance cannot be negative or zero, we can consider the k-i = a or i-j = b. As per the definition of influence distance, if a > b then a is the influence_distance otherwise b is the influence_ distance.

Here each video consists of $\{I_i , i=1,2,\ldots n\}$ image frames where ***n*** is the total number of image frames in the video. Therefore,

$Video = \sum_{i=1}^{n}(image\ frame)_i + audio\ track$ ….. (2)

Each image frame has height ***h*** and breadth ***w***. Therefore,

image frame $\boldsymbol{I = h\ w}$ ……..……..….(3)

Each image frame consists of pixels with pixel values $\boldsymbol{P_{i,j}}$ where ***i***=0,1,.....,***h*** and ***j***=0,1,……,***w***, i.e.,

image frame $\boldsymbol{I} = \sum_{i=0}^{h}\sum_{j=0}^{w} P_{i,j}$.....(4)

Each pixel is surrounded by other pixels. The neighbors of a particular pixel $P_{i,j}$ is defined as

$N=\{P_{s,t}\in I , s \neq i, t \neq j, 0 < |s-i| \leq h, 0 < |t-j| \leq w\}$....(5)

Inner neighborhood N_{ij} of any pixel P_{ij} is defined as

$N_{ij} =\{\boldsymbol{P_{s,t}}\in I , s \neq i, t \neq j, 0 \leq |s-i| \leq 1, 0 \leq |t-j| \leq 1\}$..(6)

Outer neighborhood N'_{ij} of any pixel P_{ij} is defined as

$N'_{ij} =\{\boldsymbol{P_{s,t}}\in I , s \neq i, t\neq j, 1\leq|s-i|\leq 2, 1\leq|t-j|\leq 2\}$…….(7)

In the proposed process, Eq. (8) is used to get all the pixel values of the frame with respect to values of its influence circle pixels as defined by Eq. (6) and Eq. (7). Each highest value pixel of each row of the image frame, after the transformation is identified as possible pixel to embed the authentication information. All such pixels are used to securely store authentication information.

To implement the proposed randomization concept, inner and outer influence circle is used. The equation for the pixel value of $d_{i,j}$ is

$f_{i,j} = abs(\sum_s \sum_t | d_{i,j} - d_{s,t} | - \sum_u \sum_v | d_{i,j} - d_{u,v} |)$

where

i=0,1,.....,***h*** and ***j***=0,1,……,***w***

$s \neq i, t \neq j, 0 \leq |s-i| \leq 1, 0 \leq |t-j| \leq 1$ and

$u \neq i, v \neq j, 1 \leq |u-i| \leq 2, 1 \leq |v-j| \leq 2$ ……..(8)

Let us consider an arbitrary 5 X 5 matrix of image *I* as follows

Table 1. Pixel values of inner and outer neighborhood of $d_{i,j}$

5	31	7	41	20
11	59	25	10	19
10	62	25	8	34
2	27	5	57	9
1	29	18	32	17

Let us assume a sample pixel matrix with pixel values $a_{i,j}$. Using (8) we get the following pixel values

Table 2. Sample pixel values of $a_{3,3}$

12	10	11	42	06
8	09	15	08	05
9	08	09	06	04
10	12	10	40	03
07	09	08	07	02

Table 3. Pixel values within influence circles of $a_{3,3}$

$d_{i-2,j-2}$	$d_{i-2,j-1}$	$d_{i-2,j}$	$d_{i-2,j+1}$	$d_{i-2,j+2}$
$d_{i-1,j-2}$	$d_{i-1,j-1}$	$d_{i-1,j}$	$d_{i-1,j+1}$	$d_{i-1,j+2}$
$d_{i,j-2}$	$d_{i,j-1}$	$d_{i,j}$	$d_{i,j+1}$	$d_{i,j+2}$
$d_{i+1,j-2}$	$d_{i+1,j-1}$	$d_{i+1,j}$	$d_{i+1,j+1}$	$d_{i+1,j+2}$
$d_{i+2,j-2}$	$d_{i+2,j-1}$	$d_{i+2,j}$	$d_{i+2,j+1}$	$d_{i+2,j+2}$

The proposed scheme does not consider the actual image content while selecting the pixels to embed authentication information. This technique is devised to embed short text data as secret message for authenticity in spatial domain. Using the cover frame image of red color, the sender calculates pixel value matrix using (8) and extracts the hidden bits. In this scheme, each such position value is converted into a bit stream and those bits are stored sequentially using the 7th bit of the pixel value of Red color channel of each of the pixels, starting from the first pixel of the applicable row in the even numbered image frame.

A. ALGORITHM

Step 1:Read the video

Step 2:Read Authentication information

Step 3:Convert Authentication information into Binary

Step 4:Split the video into Image and Audio

Step 5:Split each Image into image frames

Step 6: Do step 7 to step 12 untill end of all images

Step 7:Convert the pixel values of each frame using proposed conversion Eq. (8)

Step 8:Find highest value of each row

Step 9:Embed Authentication information bit in 7th bit of the highest value

Step 10:Embed Authentication information bit location in the next frame

Step 11:generate a random number and embed that number in the last row of both the frames

Step 12: goto Step 6

The ratio of the data which is communicated and the distortion which is introduced is called embedding efficiency. We get the proper definition of *embedding efficiency*, as per [11]. The maximum embedding efficiency of a arbitrary bit-stream insertion and uniform distribution of 0's and 1's using LSB interchanging method is 2. So the embedding efficiency of the proposed method is also 2.

IV. RESULTS AND DISCUSSION

We are using randomization concept with modified LSB embedding which will enhance the time complexity as well as computational complexity at a marginal limit. The time complexity of finding values of $f_{i,j}$ using (8) is O(nlogn) and the time complexity of LSB is O(n). So time complexity of this proposed method is O(nlogn) + O(n)= O(nlogn).

As time complexity of the proposed system is increased, security of the system also increased. We used 50 different uncompressed videos from Archive.com to test this algorithm. The results clearly established that the proposed force-induced pixels based video watermark process is resistant to different attacks and gives the optimal imperceptibility. For interpretation and presentation of the results here, as samples, we have used two files and the same are detailed below. The proposed method of hiding the message bits using LSB is because of its simplicity. Also the proposed method's time complexity is O(nlogn) whereas DCT, DFT is having time complexity as $O(n^2)$. Above all LSB is a lossless embedding method which gives high embedding efficiency.

As the proposed process is keyless, no overhead for key exchange is required which ensures data security. The locations of pixels are selected randomly for embedding. Different statistical analysis proves that the keyless embedding process is secured compared to embedding process with Key.

Robustness refers to maximum data amount that may be hidden into the host video without fidelity losing. Using our proposed method, we will be storing the authentication information in every alternate frames and also random number for each frame as two levels of authentication.

We have used StirMark [16-18], which is a standard benchmark tool for checking whether the steganographic and watermarking algorithms used on the image is robust or not. The attack simulates image distortions that generally take place when an image is photocopied, printed or rescanned there will be some distortions after photocopy/reprint/rescan in the resultant image. StirMark simulates image distortions of that type and checks whether the distorted image is robust or not. We executed StirMark 4.0 on the image frame and the result shows in Table 4 that shows none of the test are failed. So the proposed embedding process is robust.

Table 4. StirMark result for robustness

Name of the test	Value of Distortion	PSNR	Resultant Noise(dB)
Test_MedianCut	3	173.46	40.1901
Test_MedianCut	9	173.26	34.1105
Test_SelfSimilarities	1	172.57	41.0251
Test_SelfSimilarities	3	172.69	39.2516
Test_RemoveLines	10	172.822	NA
Test_RemoveLines	50	172.722	NA
Test_RemoveLines	100	172.824	NA
Test_Cropping	1	205.37	NA
Test_Cropping	20	197.739	NA
Test_Cropping	75	179.611	NA
Test_Rescale	50	172.875	NA
Test_Rescale	200	172.793	NA
Test_Rotation	-2	159.874	NA
Test_Rotation	5	143.98	NA
Test_RotationCrop	-.5	173.18	NA
Test_RotationCrop	1	173.739	NA
Test_RotationScale	-1	173.738	20.326
Test_RotationScale	.75	173.467	23.002
Test_Affine	1	169.97	NA
Test_Affine	8	169.22	NA
Test_SmallRandomDistortions	.95	166.19	16.45
Test_SmallRandomDistortions	1.1	165.48	15.70
Test_LatestSmallRandomDistortions	.95	167.96	20.31
Test_LatestSmallRandomDistortions	1.1	167.53	19.61
Number of tests which failed	0		

By implementing Westfeld and Pfitzmann's test [12] we can prove that the proposed algorithm is resistant to first order *statistical attacks*. Also Provos et al. [14] proved that the color frequency test is not effective if the information is hidden in randomly selected pixels though it will work well if the information is hidden sequentially.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

We are not starting the hiding process from the beginning of the image frame and the proposed process of hiding is not chronological based on pixel positions, it can withstand this test.

Proposed algorithm can withstand *duel statistics test* as flipping of LSB in this test will not be effective. In our proposed method, we are using the last but one-th bit ie, 7th bit position to hide the message bit in pixels at random positions in the image.

In terms of histogram analysis, the stego image frames are found visually indistinguishable from their cover counterpart image frames.

From Figure1 and Table 5, the comparative values prove that the two frames are *very close to similarity*. Also, the difference between means of cover frame and the frame with authentication varies from .0001 to .0010, which is very small. Similarly the standard deviation of cover frame and the frame with authentication varies from 0001 to .0006, which is again very small. Both these difference value ranges show that the original frame and the frame with hidden authentication message very similar to each other.

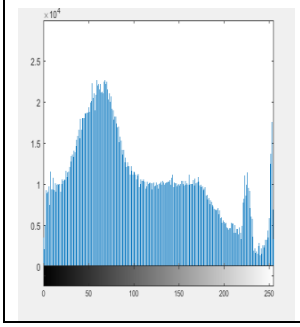
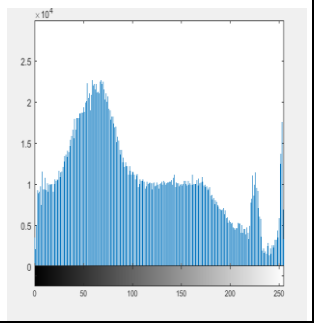
Histogram Analysis	
Original frame 5	Frame 5 with authentication information
	

Figure 1. Histogram Analysis shows the resistance to visual attack

Table 5. Comparison of two histograms of original and Image with authentication information

Euclidean Distance	Correlation	Chi-square	Intersection
$2.5902e^{-10}$	0.318	3.541	0.421

From Figure 1 and Table 5, it is clear that the cover and stego images are very similar.

If we consider the surface plots and NCC of the image frame before and after the authentication information is embedded, we find *no visual difference* from Figure 2.

Surface Plot for NCC	
Original Frame 10 and frame 10 with hidden authentication information	Original Frame 11 and frame 11 with hidden location information of hidden pixels of frame 10

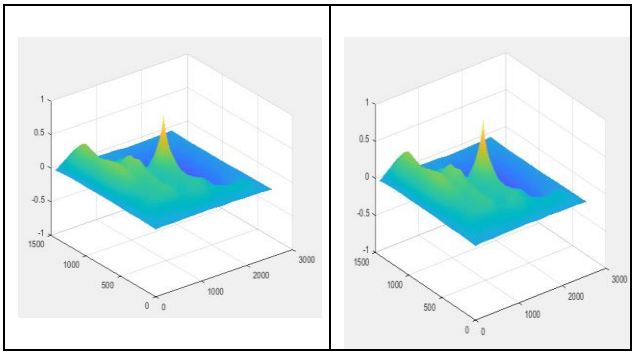


Figure. 2. Surface plots show no visual difference and proves resistance to visual attack

The hidden data is very difficult to extract which helps rise to the security of the proposed algorithm.

Also it is difficult to detect using HVS as the quality of the stego image is very high. So we can say that the proposed method can withstand visual attacks.

A Analysis through Quality Metrics

Image quality measurement – MSE, PSNR, SSIM

Mean Square Error(MSE)

MSE= $\frac{1}{M*N}\sum_{m=1}^{M}\sum_{n=1}^{N}[x(m,n) - y(m,n)]^2$, where M, N are rows and columns of image matrix, $x(m,n)$ is the original image, $y(m,n)$ is stego image.

If the value of MSE is greater than 0, then the stego image will be of poor quality.

Peak Signal to Noise Ratio(PSNR)

PSNR = 20. $\log_{10}$ [MAXPIX/RMSE] where

RMSE = $\sqrt{MSE}$ is the root mean square error, MAXPIX is the Maximum Possible pixel value of the image. If the PSNR has large value then the stego image is of good quality.

Structural Similarity Index Metric (SSIM)

SSIM = $((2a_xa_y + c_1)(2b_{xy} + c_2)/(a_x^2 + a_y^2 + c_1)(b_x^2 + b_y^2 + c_2))$

Where "a", "b", & "b_{xy}" are mean, variance, and covariance of the images, and "c_1, c_2" are the stabilizing constants. The value of SSIM will vary between 0 and 1. The value of SSIM for similar images will be near or equal to 1. As we have seen in watermark implementation using similar type of concept called energy pixel by Paul et al. [8], PSNR value is 38.62 which less than our average PNSR value 78.73. This shows that the proposed randamized pixel based steganography is better than the energetic pixel based watermark.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 7. Quality metrics of test videos

Video name	Resolution	Frames/ sec	No. of Frames	Average MSE	Average PSNR	Average SSIM
Out.avi	720X1280X3	25	125	0.0022	77.8	1
Test_1.avi	320X870X3	20	120	0.003	78.5	1

V. CONCLUSION AND FUTURE SCOPE

Here, the time complexity of the algorithm is O (*n log(n)*) indicating that it is non-computational-intensive. Experimental results show that the *PSNR* value is high, the MSE is very low and SSIM value is 1.0. Hence, we can infer that the stego image quality is close to cover image. Further, histograms show that it is difficult for the human visual to recognize any difference between a cover and Stego image frame leading to the conclusion that optimal imperceptibility is achieved. Further, as the algorithm uses every odd numbered image frame of the video to store the authentication information, robustness is implemented. We have considered authentication embedding in spatial domain only. In the sample out.avi that we used above, there were 3.69 MB of data for a very short video of duration 9 seconds. As such for full length feature films etc, data will be in big data scale. We can then consider the use of cloud for processing. We can also explore the same algorithm on transform domain.

REFERENCES

1. M. Ramalingam, "Stego machine-video steganography using modified lsb algorithm", World Acad. Sci. Eng. Technol. 74 , 502–505, 2011
2. Z. Li-Yi, Z. Wei-Dong, et al., "A novel steganography algorithm based on motion vector and matrix encoding", in: proceedings of the 3rd International Conference on Communication Software and Networks (ICCSN), IEEE, 2011, pp. 406–409, 2011.
3. Y. Cao, H. Zhang, X. Zhao, H. Yu, "Video steganography based on optimized motion estimation perturbation", in: Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, ACM, pp. 25–31, 2015.
4. H.M. Kelash, O.F.A. Wahab, O.A. Elshakankiry, H.S. El-sayed, "Hiding data in video sequences using steganography algorithms," in: proceedings of International Conference on ICT Convergence (ICTC), IEEE, pp. 353–358, 2013.
5. Deshmukh PU, Pattewar TM, "A novel approach for edge adaptive steganography on LSB insertion technique." In: proceedings of the International conference on information communication and embedded systems (ICICES) IEEE, Chennai, pp 27–28, 2014.
6. Feng B, Lu W, SunW "Secure binary image steganography based on minimizing the distortion on the texture." IEEE Transaction Information Forensics Security 10(2):243–255, 2015
7. Paul G, Davidson I, Mukherjee I, Ravi SS (2012) "Keyless steganography in spatial domain using energetic pixels." In: Proceedings of the 8th international conference on information systems security (ICISS), LNCS Springer, Guwahati, vol 7671. LNCS, pp 134–148. ISBN:978-3-642-35129-7, 2012
8. Goutam Paul, Ian Davidson, Imon Mukherjee, S. S. Ravi, "Keyless dynamic optimal multi-bit image steganography using energetic pixels" Multimedia Tools and Applications DOI 10.1007/s11042-016-3319-0, 2017
9. Cem kasapbaşi, M. & Elmasry, W. Sādhanā , "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check", Sadhana, Springer, pp 43-68. https://doi.org/10.1007/s12046-018-0848-4, 2012.
10. Singh N., Bhardwaj J., "Comparative Analysis for Steganographic LSB Variants." In:Computing, Communication and Signal Processing. Advances in Intelligent Systems and Computing, vol 810. Springer, Singapore, 2019.
11. Fridrich J, Lisonek P, Soukal D, "On steganographic embedding efficiency, information hiding." In: proceedings of the 8th international workshop, Alexandria, pp 282–296, vol 4437 2008
12. Westfeld A, Pfitzmann A, "Attacks on steganographic systems." In: Proceedings the 3rd international workshop on information hiding, LNCS 1768. Springer-Verlag, pp 61–76, 1999
13. Fridrich J, Goljan M, Dui R, "Reliable detection of LSB steganography in color and grayscale images." In: Proceedings of the ACM workshop on multimedia and security, Ottawa, pp 27–30, 2001
14. Provos N, "Defending against statistical steganalysis." In: Proceedings of the 10th USENIX security symposium, pp 325–335, 2001
15. Paul G, Davidson I, Mukherjee I, Ravi SS, "Keyless steganography in spatial domain using energetic pixels." In: Venkatakrishnan V et al (eds) Proceedings of the 8th international conference on information systems security (ICISS), vol 7671. LNCS, Springer, Guwahati, pp 134–148. ISBN:978-3-642-35129-7, 2008, 2012
16. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn. "Attacks on copyright marking systems, in David Aucsmith (Ed), Information Hiding," proceedings of the 2nd International Workshop, IH, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239, 1998.
17. Fabien A. P. Petitcolas. "Watermarking schemes evaluation." I.E.E.E. Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000.
18. http://www.petitcolas.net/fabien/watermarking/stirmar\k

AUTHORS PROFILE

Ms. Jayati Bhadra earned her M.Phil from Madurai Kamaraj University, MCA from IGNOU, M.Sc. in Applied Mathematics from Jadavpur University, Kolkata. She has nearly 16 years of teaching experience in colleges/university. She served as Coordinator of M.Sc. in computer Science and M.Sc. in Big Data Analytics at St. Joseph's. College(Autonomous) Bangalore.Her areas of research interest are Data security, Computer networks, Machine Learning and Analytics

Dr M Vinayaka Murthy, Professor Having secured Ph. D. in "Computational Fluid Dynamics - Mathematics" from Bangalore University, M.Sc. in Mathematics, B.Sc. in Mathematics from Bharathidasan University and B. Ed. degree in Mathematics from Annamalai University, he has 27 years of teaching experience in UG, PG and PhD, teaching various subjects like Discrete Mathematics, Probability and Statistics, Operations Research, System Simulation and Modelling, Finite Automata Theory, Analysis and Design of Algorithms, Computer Graphics, Data Mining & Data Warehousing, Numerical Methods, Mathematics, Basic Mathematics and Research Methodology. He is recognized by as a Research guide in computer Science of University of Mysore, VelTech University and REVA University. He has published 50 and more research papers in reputed journals and conferences. He is interested in guiding research in Data Mining and image processing. He is guiding 8 PhD Scholars. Already 2 scholars are awarded PhD in Computer Science under his guidance in REVA University;

Dr. M.K Banga, earned his Ph. D. in Computer Science from Indian Institute of Technology, Kharagpur, for his thesis on Parallel Processor Architectures. He has nearly 16 years of teaching experience in engineering colleges/university. He served as Professor of Computer Science and Systems Manager, at Bapuji Institute of Engineering and Technology, Davangere and later as Prof. and Head of the Department of Computer Science and Engineering at J N National College of Engineering, Shimoga, before joining Wipro Technologies, Bangalore. Prof. Banga served at Wipro Technologies for 14.5 years in various capacities including General Manager & Head of the Architect Academy for 2 years. He was Prof. & Head of the School of Computer Science & Information Technology for one year before joining Dayanand Sagar University. He has guided more than 15 M.Tech. Students for their project work and is currently supervising 6 research scholars for their Ph.D. degree. His areas of research interest are Data Networks, Wireless Ad-hoc Networks, Machine Learning and Analytics