
com sur™
the missing piece of CCTV
THE FOOTAGE WHISPERER
"SEE WHAT THE CAMERA SAW"
GET THE BOOK
100+ TOPICS - AIRPORTS TO ZOOS
GAUTAM D. GORADIA

UTILITY VALUE OF COM-SUR™ FOR THE BANKING SECTOR

WELCOME

AUDIT HOURS OF FOOTAGE IN MINUTES FIND OUT HOW COM-SUR, THE BEST 'MOUSETRAP' WILL HELP

"Seeing is believing - See what the camera saw"

CCTV surveillance is common in the banking sector, but footage is often only reviewed reactively. Our company realized this problem early-on and has developed the world's only CCTV video footage auditing software that encourages daily auditing (hours in minutes) of CCTV footage, filling the gap for a complete "workflow". The software works with existing cameras and VMS, regardless of type/brand, and provides a standardized approach for intelligent incident reporting. Our software also offers exceptional investigative capabilities.

'COM-SUR' – THE WORLD'S ONLY CCTV VIDEO FOOTAGE AUDITING, SMART BACKUP, AND STANDARDIZED INTELLIGENT INCIDENT REPORTING SOFTWARE – THE MISSING PIECE OF CCTV

COM-SUR is the world's only CCTV video footage auditing, smart backup, and standardized intelligent incident reporting software that serves as a complete workflow and force multiplier. It helps audit 24 hours of footage in minutes, reduces data size, creates standardized intelligent reports, and delivers business intelligence. COM-SUR helps unlock hidden information in CCTV footage and enables people to gain actionable intelligence, improve homeland security, prevent crime and losses, identify and mitigate threats and hazards, and improve operational efficiency. It empowers people to gain new jobs as CCTV video footage auditors and start new businesses of auditing video footage. Like MS Office, COM-SUR is an enabler that makes it easy to work with CCTV cameras in a standardized way, leading to better decision-making. It also offers exceptional investigative capabilities.

HOW COM-SUR SMARTLY REDUCES 'VIDEO' STORAGE SIZE

COM-SUR employs an innovative approach to

smartly reduce the amount of video to be audited and consequently the storage size of videos. Regardless of the video's frame rate, COM-SUR captures a single screenshot of the consolidated 'moment' of 'that' one second, when the I, P, and B frames come together. This method significantly reduces data size without sacrificing vital information. It goes without saying that when multiple cameras are displayed in a grid view, say 4x4, the storage size is further reduced since all the cameras are captured as a single image. Since no suggestion is being made to replace the actual video with screenshots, COM-SUR acts as a wonderful supportive technology both to audit (review) just 86400 frames representing 24 hours and reducing the data size at the same time.

BANKING SECTOR CHALLENGES

1. Thefts, robberies, and other crimes:

Banks, being custodians of ready cash and other valuables, constantly face threats of thefts, robberies, and other crimes that are a threat to the physical safety and security of the bank's employees, clients, and assets. Perpetrators often conduct pre-operational surveillance of the target area, making it important to detect suspicious activity during this phase to prevent an incident.

2. Fraud and financial crimes:

Banks are vulnerable to fraud, including identity theft, credit card fraud, check fraud, and cybercrime. Criminals may attempt to exploit weaknesses in the bank's systems or target customers to gain unauthorized access to funds or sensitive information.

3. Unauthorized access:

Unauthorized access to bank premises, such as by intruders or unauthorized personnel, can pose a security threat. This can lead to theft, vandalism, or the compromise of confidential information.

4. Physical assault and hostage situations:

Banks may face incidents involving physical assault, violence, or hostage situations. These situations can endanger the lives of bank employees and customers and require appropriate security measures to mitigate the risks.

5. Security of customer information:

Protecting the confidentiality and privacy of customer information is paramount for banks. The risk of data breaches or unauthorized access to customer accounts is a constant concern, requiring robust security measures and data protection protocols.

6. Operational continuity:

Banks need to ensure continuous operation and availability of their services. Disruptions due to natural disasters, power outages, or technical failures can impact customer trust and financial stability.

7. Insider threats:

Banks have to deal with a plethora of insider threats from disgruntled employees or even unwitting bank staff who fail to follow proper security measures.

8. Humongous growth of surveillance video:

The exponential growth of surveillance cameras has resulted in an unprecedented surge in surveillance video. Effectively managing this data has become a daunting challenge due to the massive storage capacity required,

especially considering the prolonged retention periods necessary for security, incident investigation, or legal purposes. Furthermore, the prevalence of high-resolution video with increasing megapixels compounds the storage demands, making efficient data management an urgent priority for organizations grappling with the immense volume of surveillance footage.

COVID-19 PANDEMIC

The pandemic severely impacted banks worldwide. Banks had to minimize in-person means of banking and switch to digital (online) banking instead, causing inconvenience to people who did not have means to access digital banking services. Guidelines were issued to prevent the spread of COVID-19, but outbreaks still occurred.

USE OF VIDEO SURVEILLANCE AT BANKS

Most banks have video surveillance covering the following areas:

- Entrances and exits (gates)
- Vaults and cash handling areas
- Teller counters
- Interior corridors
- Common building hallways
- Elevator lobbies
- ATMs
- Back offices and server rooms
- Parking lots

Bank personnel carry out analysis of recorded CCTV video footage of the bank branch/ATM which has been found to be useful in identifying perpetrators of crimes, resolving customer disputes, as well as in investigating and resolving crimes. Further, some banks have even begun to employ video surveillance for the purpose of studying customer behaviour as well as their satisfaction levels.

MICRO-EXPRESSIONS

Recently, some banks in India have started training employees to detect customers' lies by analyzing their facial expressions during high-value loan interviews. By using a high-speed camera to capture 200 frames per second, they aim to spot micro-expressions that occur within 1/15 to 1/25 of a second. This technique, devised by Paul Ekman, involves studying various cognitive cues such as facial muscle twitches, blinking rate, eyelid tightening, inner eyebrow raising, cheek raising, and lip nibbling.

LIVE MONITORING – CHALLENGES

Several banks have a dedicated control room with operators, set up for live monitoring of CCTV cameras. However, live monitoring comes with its own set of challenges of video blindness, poor attention span, boredom, operator bias, false alerts, and so on.

Moreover, these cameras continuously capture and record humungous amounts of video data. It therefore becomes a daunting task for the operators to review and analyse this data whenever the need arises. Thus, it may be noted that benefits from video surveillance systems can accrue only when they are used optimally, suggestions for which are

enumerated further on, in this document.

COMPLIANCE - GENERAL

Conformity or compliance in any organization means adherence to laws and/or rules and regulations, various standards, as well as data storage and security requirements as laid down by government bodies, governing bodies of the respective industry, or the management of the organization. When an organization complies with the requirements mandated by government and/or governing bodies, then it is termed as 'regulatory compliance' which enables the organization to run in a legal and safe manner.

COMPLIANCE - AUDITS

Several organizations carry out compliance audits on a regular basis to avoid the potential consequences of non-compliance.
A compliance audit examines how well an organization adheres to compliance requirements. Some organizations use video surveillance to monitor compliance issues and audit recorded CCTV video footage from time to time for investigating and preventing compliance issues. Auditing CCTV provides actionable insights on the level of compliance within the organization.

AUTOMATED SOFTWARE – WHY THEY WILL NOT WORK IN ISOLATION

In the wake of the Christchurch shooting incident, several high-profile places of worship considered deploying gun detection technology. However, there are concerns about its efficacy, since it may not be able to detect all types of weapons, or the perpetrator could still create damage before being detected.

Similarly, automated systems like video analytics, AI/ML can only detect what they have been programmed for. What about the rest? Again, these technologies are prone to triggering huge amounts of false alarms.
Also, since the permutation combinations of exceptions can be vast and varied, it becomes almost impossible to automate every kind of exception. Facial recognition technology also raises ethical and privacy concerns, and has been found to produce inaccurate results, especially for certain ethnic groups.
Therefore, experts suggest that while automated technologies will continue to grow, human intervention and intelligence will still be necessary to verify alerts and ensure their efficacy.

"CCTV IS NOT ENOUGH – WE MAKE IT WORK FOR YOU"

While it is not being suggested that optimal usage of video surveillance can cure all issues, several issues of the following kind can be addressed by doing just a little 'more' with respect to making the optimal use of video surveillance systems:

- Fraud/loss/corruption/theft

- Insider job/security lapses

- Recces/suspicious movements/activities

- Unauthorized/unlawful activities/visitors

- Entry into forbidden/restricted/no-go zones

- Workplace violence/harassment

- Staff issues

- Compliance issues

- Housekeeping issues

- Inattentive staff (e.g. guard sleeping)

- Health and safety issues

- Camera/recorder malfunctions

So, what is the 'more' that needs to be done?

1) AUDIT CCTV VIDEO FOOTAGE DAILY AS A STANDARD OPERATING PROCEDURE

'Auditing' means 'seeing' what the cameras 'saw'. Auditing of CCTV footage should be done daily (continuous investigation) to identify potential issues and threats. Auditing is a dedicated and systematic process that helps address challenges related to live monitoring and alert-based systems. Auditing helps in evaluating analyzing incidents to improve existing policies, procedures, and processes. Concerned personnel should be trained to become CCTV video footage auditors, and the audit teams should be rotated to avoid complacency/collusion. Daily auditing of CCTV footage can also help in adhering to the principles of Kaizen and TQM for business improvement.

2) DOCUMENT AUDIT FINDINGS/INCIDENTS

Audit findings/incidents should be documented in a standardized template to find the root cause to prevent future recurrences. Historical data of such findings/incidents can reveal patterns that can help take better informed corrective and preventive action. If all banks report incidents in a standardized template, relevant authorities can derive business intelligence from the data and take action for the collective benefit of the banking sector.

3) ENSURE DISASTER RECOVERY OF CCTV VIDEO FOOTAGE – LIKE A 'BLACKBOX'.

CCTV video footage must be stored at multiple locations in order to ensure that even if the recorder is stolen, destroyed or tampered with the data is never lost. Further, any backed-up data must easily be searchable and retrievable; else, it is going to be a nightmare finding the relevant video.

4) DISPLAY DYNAMIC INFORMATION AT RELEVANT PLACES

Document and display details of information that is dynamic in nature in relevant areas. For example:

1. List of authorized staff (with their duty timings and their allotted locations).

2. List of authorized external visitors (contractors, suppliers etc.)

3. List of authorized security guards (with their relevant details).

5) USE A POWERFUL NEW SIGNAGE

"WE AUDIT CCTV VIDEO FOOTAGE EVERYDAY".

One size, one color, one powerful message. Across the nation.

DE-CENTRALIZED SURVEILLANCE + CENTRALIZED SURVEILLANCE = OPTIMAL RESULTS

Organizations with multiple locations struggle with centralized video surveillance due to

infrastructure cost, internet bandwidth, and operator limitations. De-centralized surveillance offers higher accountability at each location and better situational awareness, leading to more chances of discovering exceptions.

CONCLUSION

"You see, but you do not observe" is a quote by Sherlock Holmes in A Scandal in Bohemia (1891, written by Sir Arthur Conan Doyle).
COM-SUR makes 'observation' far effortless and effectual leading to superior results.

"Cameras don't lie" - but how will you know unless you 'see' what the cameras 'saw'?
Audit CCTV - why suffer!

Get award-winning COM-SUR now. Don't wait for things to go wrong!

Finally, allow us to present three important mantras that change the landscape of video surveillance:

1. Auditing is fundamental – everything else is peripheral.

2. Cameras have lenses – humans have eyes.

3. Let's make cameras 'accountable'.