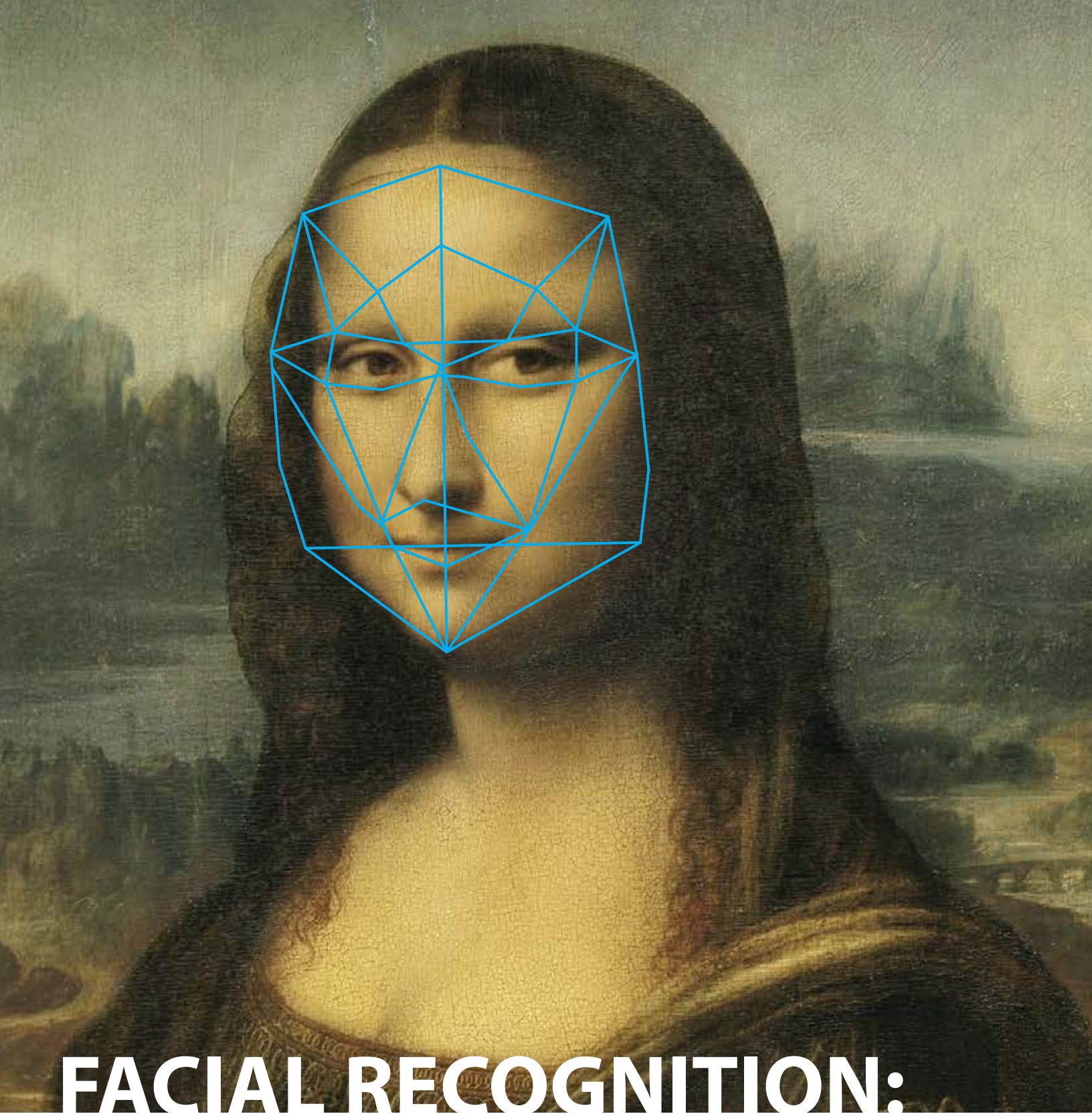


FACIAL RECOGNITION:

ART *or* SCIENCE?

VIGILANT SOLUTIONS

Facial Recognition – Art or Science?

Both the public and law enforcement often misunderstand facial recognition technology. Hollywood would have you believe that with facial recognition technology, law enforcement can identify an individual from an image, while also accessing all of their personal information. The "Big Brother" narrative makes good television, but it vastly misrepresents how law enforcement agencies actually use facial recognition.

Additionally, crime dramas like "CSI," and its endless spinoffs, spin the narrative that law enforcement easily uses facial recognition to generate matches. In reality, the facial recognition process requires a great deal of manual, human analysis and an image of a certain quality to make a possible match. To date, the quality threshold for images has been hard to reach and has often frustrated law enforcement looking to generate effective leads.

Think of facial recognition as the 21st-century evolution of the sketch artist. It holds the promise to be much more accurate, but in the end it is still just the source of a lead that needs to be verified and followed up by intelligent police work.

Today, innovative facial recognition technology techniques make it possible to generate investigative leads regardless of image quality.

Part science and part art, these techniques offer your agency the opportunity to cut through the frustration and generate higher-quality leads to protect the communities you serve more effectively.

Roger Rodriguez joined Vigilant Solutions after serving over 20 years with the NYPD, where he spearheaded the NYPD's first dedicated facial recognition unit. The unit has conducted more than 8,500 facial recognition investigations, with over 3,000 possible matches and approximately 2,000 arrests. Roger's enhancement techniques are now recognized worldwide and have changed law enforcement's approach to the utilization of facial recognition technology.

VIGILANT SOLUTIONS

The Science

Terms to Know

This paper will go into great detail on the facial recognition process and how you can leverage it to generate leads for your agency. For background, here are some important terms for you to know:

Facial Recognition: An application that uses biometric algorithms to detect multiple landmarks and measurements of a face that may be compared to a gallery of known images to find potential matches.

Facial Identification: The manual process (the human aspect) of examining potential matches from facial recognition, looking for similarities or differences.

Face Print: A digitally recorded representation of a person's face that can be used for identification of the person based on unique characteristics. Also known as a Face Template.

Algorithm: A process or set of rules to be followed in calculations, or other operations, which is set by a computer. In facial recognition the algorithms are rules on how to read a face.

Gallery: Any database of known images. Gallery images can come from a number of sources, including mugshots, watchlists or hotlists.

Probe Image: Any unknown image captured for facial recognition. Probe images can be taken by an officer in the field using a camera or mobile phone or from other sources such as security and CCTV cameras.

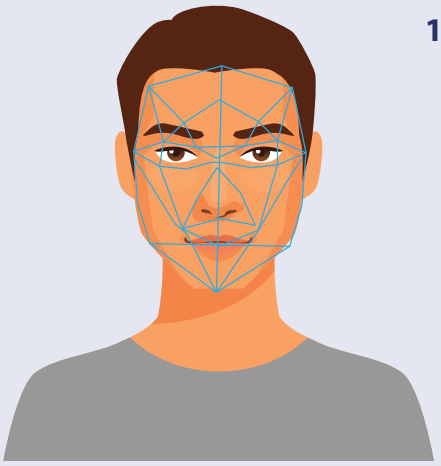
Gallery Image: An image from an existing facial recognition database. Once a probe image is run through the facial recognition system, it is manually compared to gallery images to identify potential matches.

Controlled (Constrained) Images: Images with good lighting, frontal face positioning, high resolution, and acceptable distance from camera (examples: taken by a field officer, kiosk station, identification card photos). Controlled images are optimal for facial recognition matching.

Uncontrolled (Unconstrained) Images: Images with poor lighting, poor poses (looking down or up, and certain profile captures), low resolution, heavily pixelated, overexposed, underexposed, subject is too far away, fisheye camera captures, distorted or skewed images, pictures or recordings of a screen, photocopies with excessive noise, or occlusion (blocking any part of the face).

How Facial Recognition Works

How Law Enforcement Uses Facial Recognition



1. Gallery created by capturing or uploading mugshots.

2. Probe Image is uploaded to the facial recognition application.

3. The algorithm creates a Face Print of the Probe Image.

4. Facial recognition compares the Probe Image against the Gallery.

5. Facial recognition application returns a list of possible matches.

Just as important as the technology that makes up the system are the individuals who use it. The human element of the facial recognition process remains essential to getting a possible match and generating a valuable lead. The success of facial recognition depends on agencies that know how to leverage a system's strengths against lower picture quality.

Best Practices

Probe Photos, Gallery Images and Image Submission

One of the most important rules of facial recognition matching: The accuracy of the facial recognition application depends heavily on the initial quality of the image. For that reason it is paramount to gather controlled probe and gallery images.

Field Officer Image Capture

When a field officer captures a photo for facial recognition from a camera or smartphone, the objective is for the image to resemble a standard mugshot in pose, distance, and lighting. With that in mind, here are best practices for image capture:

1. **Officer safety** is paramount. It is advised to use judgment on when and where to capture the photo.
2. The field officer must **control the photo capture,** not the subject.
3. Capture the photo from a **distance of 2–5 feet** away from the subject.
4. The **subject must face forward** with eyes looking straight ahead. No head tilts.

Agency Booking Officer Mugshot Capture

When an Agency Booking Officer captures an image for a mugshot, the following are considered best practice recommendations for mugshot (gallery) images to work correctly with facial recognition:

1. **Background:** Should be plain in color. Preferably gray but generally a solid color.
2. **Lighting:** No dimly lit areas. Lights need to be bright enough but not to cast shadows on a face.
3. **Pose:** Subject must look straight ahead and be aligned with the camera. No head tilts.
4. **Facial Expressions:** No smiling or exaggerated facial expressions on the subject.
5. **Hair:** Should not cover the inner part of a face. This area is considered to be 2 inches above the eyebrows, down to the chin, and ear to ear. This area must be unobstructed and clear for effective captures of mugshot images.
6. **Right and Left Profile Captures:** Recommended to assist in facial identifications by providing the analyst or investigator multiple views of a candidate during the review process of probe-to-candidate comparisons. Facial features may present themselves in the added profile image that may have otherwise been missed before, such as scars, marks, or tattoos. Ear structure and lobe patterns are as unique as fingerprints. These physical identifiers are exclusive to the individual. In addition to frontal images, profiles provide valuable information in the identification process by showing definitive similarities or differences between two people.

VIGILANT SOLUTIONS

Best Practices
Probe Photos, Gallery Images and Image Submission

Going one step beyond the booking photo process, gallery management is critical to the probe-to-template match relationship in facial recognition. If possible, retake bad images to ensure proper data management. Doing so will result in clean databases, which are critical and lead to higher accuracy rates in facial recognition.

Submitting Existing Images or Video

When submitting an already existing image or video for facial recognition, initial recommendations include:

1. Submit **original, uncropped images** and original videos.
2. Submit **proprietary codecs** when applicable. If not, the analyst/investigator will not be able to retrieve a still image from the video for facial recognition.
3. If possible, **do not take pictures of an image or of a computer screen** playing a video.
4. If possible, **do not record videos from a phone** or other device.

Note that it is not always possible to adhere to all of these recommendations for various reasons. However, not doing so impacts the quality of the images and will ultimately hinder the performance of any facial recognition application during a search.

Image Analysis

Once you submit an image for facial recognition analysis, the analyst's or investigators' initial responsibility is to evaluate or triage the probe image. They must answer two questions:

1. **Does the probe image meet the criteria for facial recognition searching?**
2. **Does the probe image need pre-processing with image enhancements?**

If the probe image meets the criteria for facial recognition searching, the image is classified as a controlled or high-quality image, and proceeds to facial recognition searching. If the probe image needs pre-processing, then the image is most likely uncontrolled and of lower quality, and one or more factors exist that make the inital probe image ineffective for facial recognition searching.

In the past, an uncontrolled classification meant the investigator could not conduct a facial recognition search. Today, new approaches in image pre-processing, and easy-to-use enhancement tools, make it possible to make lower-quality images acceptable for facial recognition searching. These enhancements are changing the paradigm in the facial recognition process by expanding its effectiveness as a lead generator in the space of public safety, and will be explored in greater detail later in this paper.

Once a probe image has met the criteria for facial recognition, either initially or through image enhancements, the investigator enrolls it into the facial recognition application for searching against any galleries available from the agency and/or commercial sources.

The Facial Recognition Search: Probe-to-Template Matching

When the investigators enter the probe image into the facial recognition search, the applications' biometric algorithms detect multiple landmarks of the face and then compare it to a gallery of images to find potential matches.

To return a possible match using facial recognition, a probe image must have an associated database image.

Therefore, an individual that does not have a pre-existing mugshot residing in the gallery will **NEVER** return in a facial recognition search. Similar-looking candidates may display, but the true candidate will never appear. No matter how good the probe image appears to be, the association will never be made. **True probe-to-template matching is completely dependent on the union of two images, a fact often overlooked by media outlets and Hollywood, but incredibly important to note in any discussion of facial recognition and its implications on privacy.**

VIGILANT SOLUTIONS

The Facial Recognition Search: Image Quality

When analysts or investigators enroll a probe, they should align their matching accuracy expectations with the initial image quality of the probe. If they enroll a high-resolution probe, the candidate will often return higher in the candidate return list. If they enroll a low- to medium-quality probe, the return will most certainly reside deeper in the candidate list.

Low Resolution Image

High Resolution Image

Why? Images with lower resolution have data loss. When data is missing, it significantly impacts the ranking. Simply put: More data = a higher ranking, less data = a lower ranking. Because of this, an analyst should never expect a Top 10 ranking on lower-quality probes. When enrolling an image with lower resolution that returns lower rankings, analysts should:

- Expand the gallery and standardize the return list between 200–500 candidates, as a candidate may reside deeper in the return list.
- Utilize filters that are built into the GUI of most systems. Filters read the metadata behind each gallery image. They also act as a process of elimination for larger databases. When looking for a known gender, race, or location, applying filters to a search only helps to narrow a list of candidates, and substantially drives the results to smaller groups of specificity. Properly using filters for lower resolution probes only increases the likelihood of obtaining a possible match residing in your list of candidates, because you are leveraging the metadata to work in tandem with facial recognition algorithms.

When the probe is of lower quality, analysts need to become more actively involved in the facial identification process.

The Human Aspect: Facial Identification

While we have already defined facial recognition as a computer application detecting attributes of a face and matching them to a gallery, it significantly differs from facial identification.

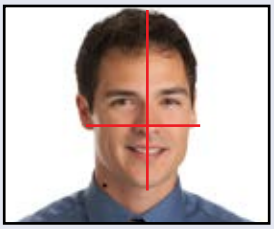
Facial identification includes the manual process and human counterpart. The identification process is purely visual. Analysts should always be in the habit of examining facial images, looking for both similarities and differences.

Unfortunately, many analysts opt to allow the system to perform the search and return results and are often disappointed when a match is not made. But analysts should know that a sole reliance on the facial recognition application for a match tends to work when searching with controlled photos.

With uncontrolled images, analysts and investigators must manually analyze images, working in tandem with the facial recognition application. It is just as critical to the process and is always necessary when working with lower-quality images. **Don't rely solely on the facial recognition application!**

The Analysis of a Face: Probe-to-Candidate Comparison

When particular faces become of interest to the analyst/investigator, the analysis process becomes more detailed and methodical. Performing a visual scan of faces will automatically eliminate candidates quickly, allowing an analyst/investigator to navigate through larger candidate lists rather easily. Several strategies and areas of focus are recommended to more efficiently make use of time during the identification process:



1. **Analyze the ears and hairline** on all the returned candidates. Ears are unique. Lobe shapes on frontal images are easily identifiable and lobe patterns on profile images are as distinctive as the fingerprints on a hand. Even receding hairlines maintain levels of consistency with patterns, and fuller sets of hair have unique parts such as widow's peaks or may display a particular ethnic hair type.

2. **Divide a face into four quadrants.** Top left, top right, bottom left, and bottom right. When conducting a visual comparison of probe to candidate, the analyst or investigator must carefully review both, looking for similarities and differences in each.

3. **Look for "locks" or certainties** that may exist between probe and candidate. These validate the physical characteristics between both images and assist in the identification process during peer review. These locks may be found in disfigurements, scars, moles, piercings, hairlines, tattoos, etc.

Once satisfied with a particular candidate, an immediate background investigation is advised. Once the candidate's physical characteristics have been satisfied in the identification process, the validation process begins. Check for incarceration status, criminal background, residences in relation to the crime location, and modus operandi. Careful review and analysis of these factors strengthens the investigation and will solidify or discredit your potential possible match candidate.

Facial Recognition is not an absolute science. It is not quantifiable like DNA, so any and all intelligence information gathered on your candidate will greatly contribute to the greater good of the investigation by making your single choice a strong investigative lead.

Once you obtain all information, it is recommended that a peer review analysis be conducted in your agency. This can involve colleagues and should be no more than three to five persons in total.

VIGILANT SOLUTIONS

Art Meets Science

Advances in Technology and Processing Techniques

When it comes to facial recognition, the greatest challenge to law enforcement is the fact that most probe images obtained by law enforcement are uncontrolled in nature. They often originate from off-axis CCTV camera feeds, low-quality ATM photos, social media images and other sources where the image is less than ideal for facial recognition. Most present-day facial recognition systems cannot read medium- to low-quality probes. In order to overcome these limitations, Vigilant Solutions created its suite of specialized facial recognition enhancement tools. These easy-to-use tools enable analysts and investigators to enhance select lower-quality images that previously could not meet the criteria for facial recognition searching. They can include certain images with:

- Poor lighting.
- Poor subject poses–looking slightly down or slightly up, and certain profile image captures.
- Low Resolution.
- Heavy pixelation.
- Overexposure.
- Fisheye effects.
- Distortion or skewing.
- Occlusion (any part of the face blocked or covered).

These pre-processing image enhancements are made following the probe image analysis discussed earlier. Once complete, and the probe image meets facial recognition searching criteria, investigators can enroll it into the application for searching against the gallery. **Pre-processing enhancements simply raise the probe image facial recognition quality to levels conducive for searching.**

Tip: Distorted or skewed images will return results with the same shape. Pre-processing the image can yield better results.

VIGILANT SOLUTIONS

Breakthrough Technology Improves Match Odds

A breakthrough in the public safety space and a new direction in the facial recognition process involves the manual graphic enhancement of images. In this case, the eyes are graphically placed over the original probe image. This important yet simple enhancement technique changes the entire dynamic of the search. The method of probe-to-template matching remains consistent – looking for similarities – and now the candidates returned all have eyes opened. In this case, the best candidate match even ranks first. The underlying method of manually inserting the eyes over the existing image is graphic design at its best. Yet it proves once again: More data = a higher rank, and gives credibility to the statement, "Facial recognition is part art, and part science."

Art and biometric science combined with graphic design elements increase the odds of finding potential matches. This simple trick of adding eyes dramatically raised the quality of the candidates returned. More importantly, it also provided the best possible match in the gallery at rank one. The eye placement does not have to be exact nor is eye color an issue. Manually adding the eyes allows for the algorithms to make the proper measurements on the face, many of which are in relation to eye placement.

This single technique has been extremely effective in leveraging the algorithms behind the facial recognition software and has returned candidate matches hundreds – if not thousands – of times. It also proves to users that combining art and science in facial recognition provides additional options to leverage the true power of this technology.

Tip: Eyes are like the cog to the facial recognition wheel.

Pre-Processing Tips and Tricks

Pre-processing image enhancements can be performed with many popular image editing software applications; however, most do not document a user's enhancement history. To maintain integrity within any facial recognition search, use facial recognition software with built-in enhancement tools.

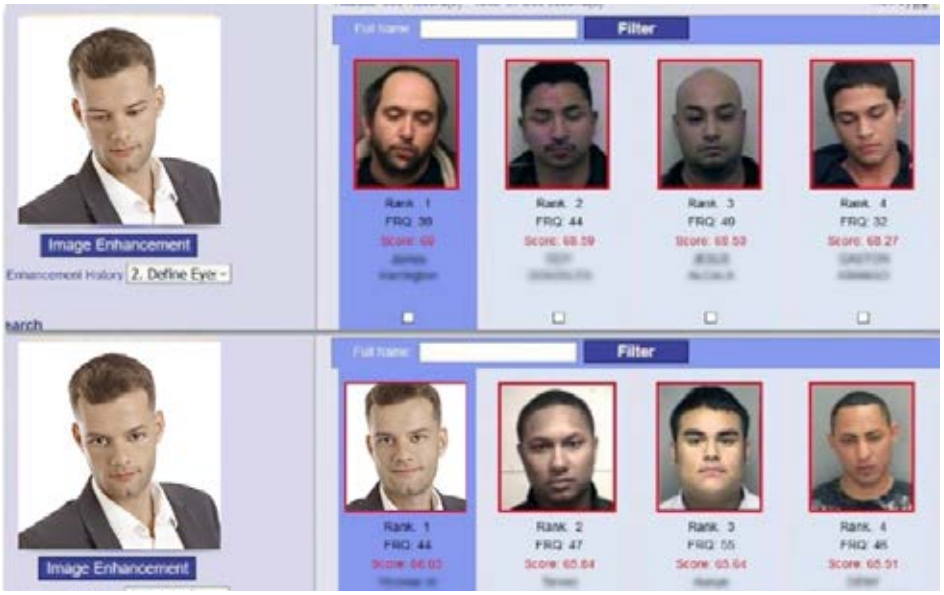
All image enhancements should be documented historically for integrity and case management. Because there are other image editing applications currently available in the market, documentation is strongly encouraged when using these tools as well. While courtroom testimony does not require documentation at this time, good documentation shows analysts are acting in good faith throughout the facial recognition process. Further, the documentation validates how the software and investigative process provided a solid investigative lead.

Built-in enhancement tools for a facial recognition system enable analysts to leverage the system for a greater advantage. Having a trained eye to identify potential problematic images is also critical to the process. The following images are examples of what to look out for when performing facial recognition searches for your agency.

Eye Placement: The Eyes Have It!

Facial recognition systems rely heavily on predetermined eye locations to properly orient the probe face before a search against the gallery. **Eye positions and placements are the root of any facial recognition search. The matching process begins with the eyes, and the algorithm reads the face systematically thereafter.** Because of this, eye capture and placement is critical. The eyes represent the cog on the facial recognition wheel–a centralized focal point allowing the recognition process to work around it. For most images that are controlled and higher in resolution, facial recognition applications tend to select the eye placements automatically. The same cannot be said for uncontrolled, lower-quality images. It is critical that an analyst be able to identify situations where manual eye placements are needed, especially on probes of lower quality.

There are instances where a person's nostrils will be mistaken for eyes. This normally happens when human heads are positioned looking slightly upward, and the nostrils are found to be more prevalent within the photo.

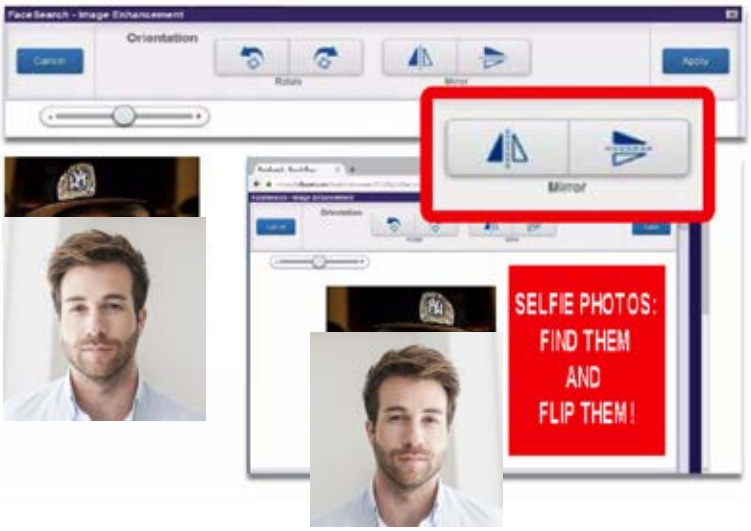


If the analysts rely only on the software, the matching ability is severely compromised right at the start of the search. Manually placing eyes on a photo takes the guesswork out of the application and maintains the integrity of the search, but only when the analyst establishes careful analysis and implements a routine.

You can see the importance of eyes in the facial recognition process in the relationship of the probe to candidate by examining the contents of listed results after a search is performed. The image above shows the dynamic power of the eyes for facial recognition software. The top photo shows what happens when a probe image is introduced to the system with closed eyes. The results in the candidate list will certainly appear same. Most, if not all, of the candidates have eyes partially or fully closed. This should be expected, and is a prime example of the probe-to-template matching process looking for similarities between both images.

Mirroring: The "Selfie" Probe Image

Certain images taken with cell phone cameras are "mirrored." This causes the facial recognition algorithm to "read the face in reverse." Enhancement tools allow a user to correct the problem. For example, with Vigilant Solutions' FaceSearch™ product, you can select the orientation feature and use the Mirror tool to correct the "mirrored" pose of the probe. This brings the image to a "natural" state and allows the algorithm to read the face effectively. This enhancement is then contained in the audit trail of the probe image for later review and discovery.

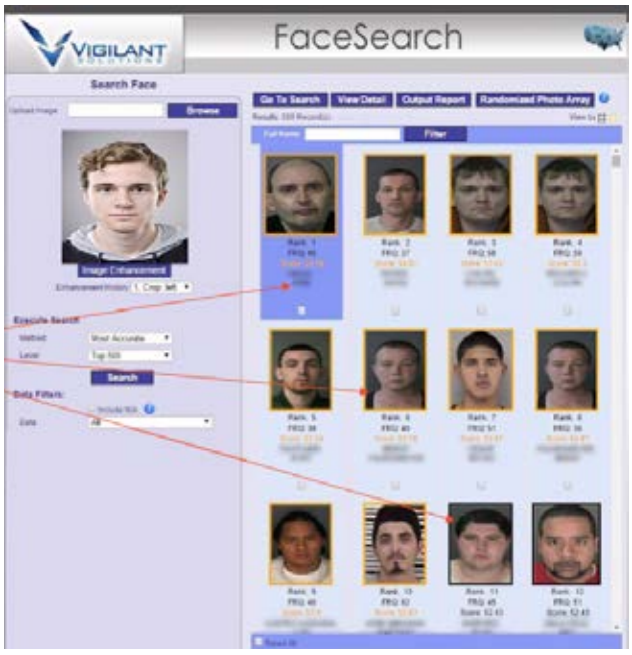


Use pre-processing tools to identify telltale signs within a probe photo. Identify letters, text, or emblems, and determine if they are in reverse. Once you flip the probe photo horizontally and the orientation reads true, search the enhanced probe against the gallery and see the results.

Tip: Look for the "selfie" images that are mirrored. Be sure to flip them.

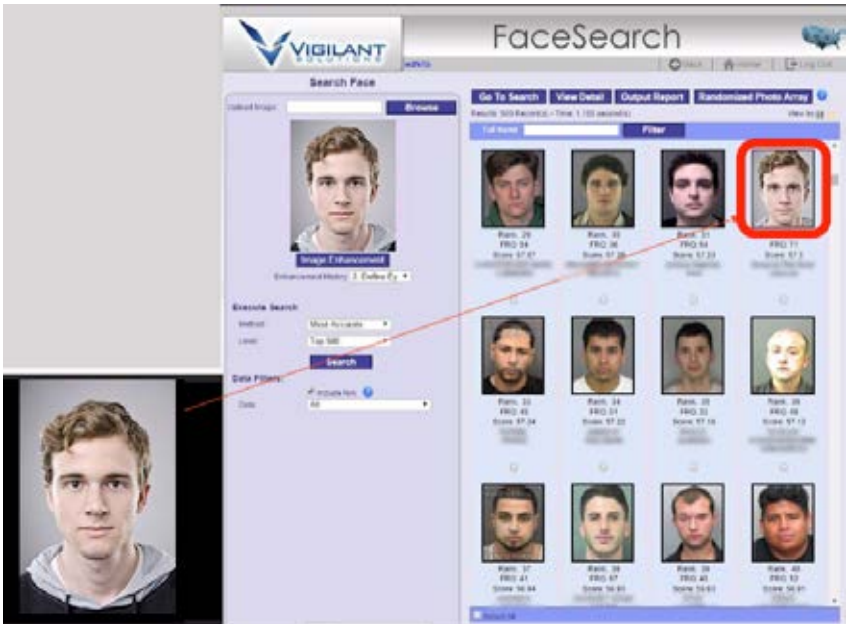
Image Distortion: The Fisheye Effect

There are times when an analyst may have to work with a probe photo that is severely distorted or skewed. Some images may have a fisheye effect. These images may come from ATM machines, bank surveillance cameras or from a CCTV camera. These images in their current state cannot be accurately read by the facial recognition software because the "face" is not true to scale. Many analysts will extract the image and perform a search, and will fail to get a result that looks anything like the probe image.



The algorithms return candidates with similar-shaped faces. Most of the candidates have skewed or distorted images.

In this situation, remember the proper use of enhancement tools. These images need pre-processing enhancements before they can be searched. Here, the images returned candidates with similar-shaped faces, and most of the candidates are also skewed and distorted. Analysts must be able to identify these images and "correct" them to return better candidates in facial recognition searches.



The corrected probe image returns the image to a more "natural" appearance with enhancement tools, and the algorithm returns better candidates in probe-to-template matching.

Image Distortion: Every day, facial recognition analysts face uncontrolled image problems such as image distortion, or the fisheye effect, and mirroring. Identifying these problematic probe images and knowing when to use enhancement tools will definitively change the dynamic of search results and will lead to more credible possible match results.

VIGILANT SOLUTIONS

Facial Recognition Matches as Investigative Leads

It is important to note that ALL facial recognition matches are classified as possible matches. When a search returns a candidate, analysts must validate the true probe-to-template matching with a visual validation in the identification process. From there they must determine if the match is strong enough using further intelligence-driven assessments. The peer review process then reviews and validates both the probe and the candidate a second time.

Since facial recognition is not a science, nor is it regulated, and there are no restrictions in place, it cannot be deemed as absolute, and all matches remain POSSIBLE. Even after performing due diligence in the investigative process, the end result of any facial recognition analysis must provide analysts with a very good investigative lead. Any enhancements analysts make during image pre-processing represent a good faith effort to triage lower-quality photos in an attempt to leverage the technology to generate a potential lead.

Compare this process to a caller phoning into a particular law enforcement agency and stating he has just seen a suspect wanted for a particular crime on the news. He further states that he recognizes the perpetrator, and also provides a location for finding him. The caller provided the agency with potential intelligence information. The responding agency official does not have a right to effect an immediate arrest. Probable cause must be established from this potential lead before an arrest is made. The onus falls on the investigator to establish probable cause from the information provided to make the lead credible, and eventually make an arrest.

The same standard applies to facial recognition, and all matches resulting from any facial recognition investigation. The onus continues to fall on the agency to verify a person's true identity independently from the facial recognition application. Other standard law enforcement procedures are still required to establish probable cause for an arrest. The agency must never base the arrest solely on a facial recognition match. The technology, even with the remarkable advancements that have been made, should only be viewed as a reliable and credible lead generation tool.

It is important for agencies and facial recognition users to understand these critical points, which should be part of the agency's facial recognition workflow and facial recognition and facial identification policy. With this level of understanding, and through proper use of available facial recognition tools, this technology can make a significant impact on an agency's criminal identification and apprehension rates.

Conclusion

The time is finally here when the promises of facial recognition can become reality. With advanced facial enhancement tools – part science, part art – applications such as Vigilant Solutions' FaceSearch™ enable law enforcement to secure high-quality investigative leads, protect personal privacy, and keep communities safe.